BITCOIN AND CRYPTOCURRENCY TRADING

The Best Crypto Trading Strategies for Beginners to Change Your Life During the 2022 Bull Run – Apply Technical and Fundamental Analysis to the Blockchain

CHARLES SWING
MASARU NAKAMOTO

VISIT…

Bitcoin and Cryptocurrency Trading

The Best Crypto Trading Strategies for Beginners to Change Your Life During the 2022 Bull Run – Apply Technical and Fundamental Analysis to the Blockchain

By

Charles Swing

&

Masaru Nakamoto

© Copyright 2021 by Charles Swing and Masaru Nakamoto

The following eBook is reproduced below with the goal of providing information that is as accurate and reliable as possible. Regardless, purchasing this eBook can be seen as consent to the fact that both the publisher and the author of this book are in no way experts on the topics discussed within and that any recommendations or suggestions that are made herein are for entertainment purposes only. Professionals should be consulted as needed prior to undertaking any of the action endorsed herein. This declaration is deemed fair and valid by both the American Bar Association and the Committee of Publishers Association and is legally binding throughout the United States. Furthermore, the transmission, duplication, or reproduction of any of the following work including specific information will be considered an illegal act irrespective of if it is done electronically or in print. This extends to creating a secondary or tertiary copy of the work or a recorded copy and is only allowed with the express written consent from the Publisher. All additional rights reserved. The information in the following pages is broadly considered a truthful and accurate account of facts and as such, any inattention, use, or misuse of the information in question by the reader will render any resulting actions solely under their purview. There are no scenarios in which the publisher or the original author of this work can be in any fashion deemed liable for any hardship or damages that may befall them after undertaking information described herein.

Additionally, the information in the following pages is intended only for informational purposes and should thus be thought of as universal. As befitting its nature, it is presented without assurance regarding its prolonged validity or interim quality. Trademarks that are mentioned are done without

written consent and can in no way be considered an endorsement from the trademark holder.

INDEX

Introduction

PART 1 - BITCOIN

Chapter 1 - The First Cryptocurrency Ever Invented

Chapter 2 - How Bitcoin Works

Chapter 3 – Wallets

Chapter 4 - Forks

Chapter 5 - Buying and Selling Bitcoin

Chapter 6 – Putting Everything Together

Chapter 7 - The Blockchain

PART 2 - THE CRYPTOCURRENCY ECONOMY

Chapter 8 - The Economics of Bitcoin

Chapter 9 - The Problem With Capitalization

Chapter 10 – Wealth Distribution

PART 3 - ALTCOINS

Chapter 11 – Ethereum

Chapter 12 - Tether and Stablecoins

Chapter 13 - Chainlink and Oracles

Chapter 14 - Uniswap and Decentralised Finance (DeFi)

Chapter 15 - Yearn Finance

Chapter 16 - Basic Attention Token (BAT) and Utility Tokens

Chapter 17 - NFTs: Another Token Standard

PART 4 - BEYOND ETHEREUM

Chapter 18 - Cardano and the Academic Approach to the Blockchain

Chapter 19 - Polkadot and the Concept of Parachain

Chapter 20 - Dogecoin and Meme Coins

PART 5 - INVESTING IN CRYPTOCURRENCIES

Chapter 21 - False Myths about Cryptocurrency Investing

Chapter 22 - The Bitcoin "Dominance"

PART 6 - ECONOMIC ANALYSIS OF CRYPTOCURRENCIES

Chapter 23 - The Capitalization of Cryptocurrencies

Chapter 24 - The Inflation Rate

Chapter 25 - Wealth Distribution

Chapter 26 - The Longevity of a Cryptocurrency

PART 7 - BUYING, SELLING AND STORING CRYPTOCURRENCIES

Chapter 27 - Choosing an Exchange

Chapter 28 – Storing your Crypto

PART 8 - INVESTMENT STRATEGY

Chapter 29 - Capital Allocation

Chapter 30 – The Dollar Cost Averaging Plan (DCA)

Chapter 31 - The Advanced Dollar-Cost Averaging Plan (ADCA)

Chapter 32 - Results of the Advanced DCA

Chapter 33 - Building the Portfolio

Chapter 34 – Portfolio Rebalancing

Chapter 35 – Cash Flow Oriented Strategies

Chapter 36 – Portfolio Overview

Chapter 37 - Monthly Process for Using This Portfolio

PART 9 – CRYPTOCURRENCY TRADING

Chapter 38 – What is Online Trading?

Chapter 39 – Fundamental Analysis

Chapter 40 – Technical Analysis

Chapter 41 – Basic Technical Analysis Indicators

Chapter 42 - Moving Averages and MACD

Chapter 43 - Linear and Logarithmic

Charts

Chapter 44 - Dow’s Principles

PART 10 - CONTROL YOUR EMOTIONS

Chapter 45 - Keeping Your Emotions Under Control

Chapter 46 - Understand your Psychology

Chapter 47 - Becoming a Better Cryptocurrency Investor

Chapter 48 - Learning from your mistakes

Chapter 49 - The Importance of Keeping a Cryptocurrency Trading Journal

Chapter 50 - Why Beginner Cryptocurrency Traders Do Not Make Money

Chapter 51 - Beware of Scams

BONUS CHAPTER: Cryptocurrency Debit and Credit Cards

Conclusion

Check List Cryptocurrency Evalutaion

Glossary

Useful Resources

References

Introduction

Bitcoin and cryptocurrencies are piquing the interest of an ever-growing number of people. You've probably heard friends and colleagues talking about blockchain, Ethereum, and more of the sort and have felt left out because you don't understand what the industry is all about. Well, we can tell you a secret: most of them have no idea what they are talking about either. You may be surprised to find out that many approach this world with a warped perspective of it and distant dreams of making money in ways that are completely detached from reality; most, in fact, "invest" (if one can even call it an investment) their money in projects they don't understand just because "cryptocurrencies are the future."

In truth, the only way to properly approach this sector sustainably is through a thorough understanding of the technological and economic foundations that govern it. This book has the purpose of illustrating the basic concepts behind cryptocurrencies and blockchain simply and clearly, through

concrete examples that everyone and anyone can understand.

That being said, this book won't be yet another eulogy of cryptocurrencies. Instead, every aspect will be treated in the most unbiased way possible to allow you to make up your mind about this topic. Cryptocurrencies are technology-based and, as such, should be studied by looking at data rather than that the fleeting emotions of a rising or falling market.

To begin, we will discuss the technological and economic structures of Bitcoin, as it lends itself to be a good starting point for the study of the blockchain. Following that, the focus will shift to Ethereum and decentralized applications (what your friends mistakenly call "cryptocurrencies" without knowing they have nothing to do with one another). Finally, the most capitalized project in each sector will be presented with a systematic and linear approach.

Although it is not this manual's purpose, by studying the contents of this book, you will also develop the necessary skills to approach

the investment side of cryptocurrencies.

Therefore it can be considered a step-by-step guide to train you if you have decided to approach this area with a certain level of seriousness for the first time (or in case you need to clear up the confusion caused by reading other similar 'guides').

Happy reading!

PART 1 - BITCOIN

Chapter 1 - The First Cryptocurrency Ever Invented

Of course, a book on cryptocurrencies must begin with the first digital currency ever invented: Bitcoin. Bitcoin is an excellent starting point since it allows you to understand the narrative and philosophy behind the industry without needing overly sophisticated theoretical knowledge. The technical side of its function, which we will see in a moment, can be complicated to understand if you do not follow a coherent and logical thread; over the following few pages, we will explain it in-depth to provide the tools to analyze and understand other significant cryptocurrencies. Let's start.

What is Bitcoin?

Bitcoin is digital money, but unlike the legal

tender currencies, we are used to, no central bank controls and regulates it. Instead, Bitcoin’s financial system is managed by thousands of computers spread worldwide: anyone who wishes to can participate in this ecosystem.

Announced in 2008 and launched in 2009, Bitcoin was the first cryptocurrency available and is still the most heavily capitalized to date. Bitcoin was created to provide the ability to send and receive digital money to and from anywhere in the world within minutes. Furthermore, since there is no central authority, it cannot be blocked, making it so attractive to its users.

Use cases for Bitcoin:

People use Bitcoin for many different reasons. Many like it for its free and uncontrolled nature: anyone with an internet connection can send and receive Bitcoin. We can think of it as a digital version of cash since no one can stop it from being used. Keeping in mind that it's a digital currency,

we can see the added interest established by allowing easy international exchange.

Some see Bitcoin as a form of investment as opposed to a simple way of exchanging money; they choose to hold on to their Bitcoins for a long time, hoping to one day sell them at a higher price than that they spent on them. These people, known as "holders," gave Bitcoin the nickname "digital gold," thanks to some properties that we will see shortly. But, for now, it's sufficient to understand that "holders" believe that these peculiarities make it an ideal means to store their wealth for long periods.

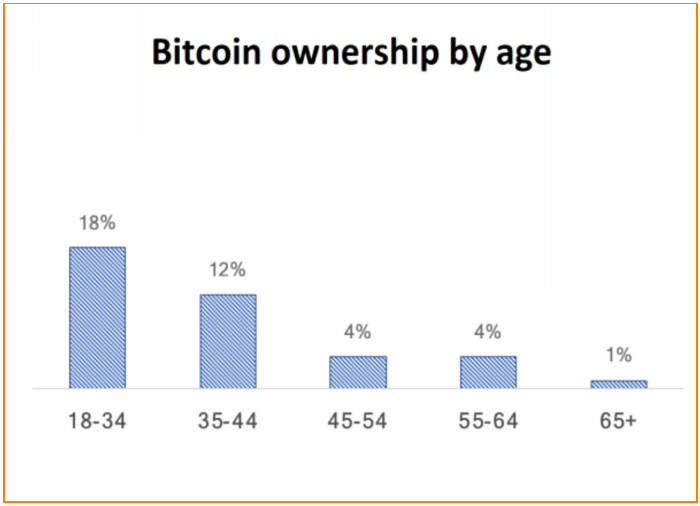
Lastly, there is a third category of people fascinated by Bitcoin: traders. They see its significant volatility as a huge opportunity to make money through speculative buying and selling. For example, on 12 March 2020, Bitcoin lost 38% of its value in a single day. Such large price swings allow traders to make significant profits.

One can therefore have a triple vision of Bitcoin:

- Transactional

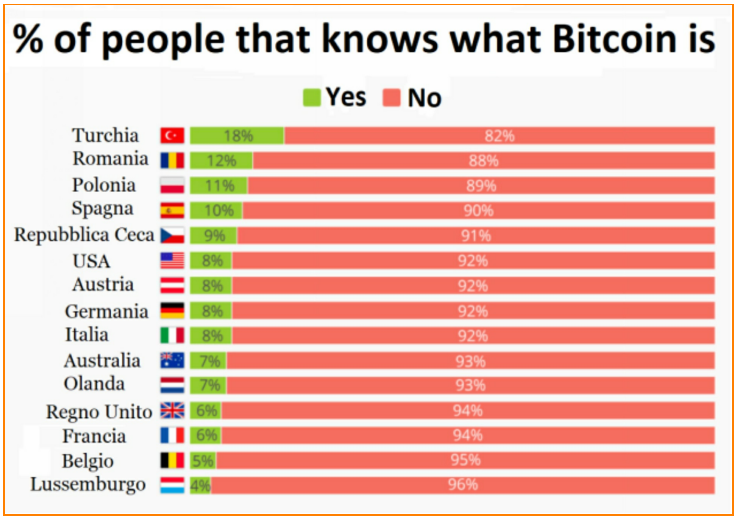
- Financial
- Speculative

The image below shows partial data on the average age of Bitcoin users. As you can see, summing the fractions does not add up to 100%: this is because Bitcoin offers the possibility to maintain a certain degree of anonymity. Therefore, as mentioned above, the available data is only partial.

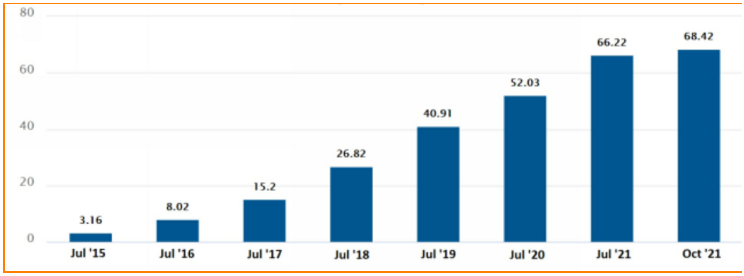


The Spread of Bitcoin

Before we get into the technical side of things, there is one more thing to mention. Although Bitcoin is spreading worldwide faster than the internet did in the early 2000s, there are still very few people who actually know about it and even fewer who possess any. As is shown in the picture, only very few people in the world know about the existence of Bitcoin (and cryptocurrencies in general); it's also impossible not to notice that in Europe, only 8% of the population knows what Bitcoin is. So, if you are reading this book, you are definitely among the first to delve into this field seriously.



An interesting aspect to note is that as the number of users increases, the price of Bitcoin also tends to rise. Of course, this is not a direct correlation, but, to date, it is a reasonably accurate proportion. The image below shows the number (in millions) of participants in the Bitcoin network: you can see a relatively steady growth year after year.



Likewise, the graph showing Bitcoin's price changes since 2014 follows this trend relatively similarly.

Now that we have clarified Bitcoin's different uses, its spread, and its relationship with its price, let's look at how it works.

To recap

- Bitcoin is a digital form of money that does not rely on a central entity.
- There are three types of people who use Bitcoin: speculators, investors, and those who use it as a payment method.
- In Europe, only 8% of the population knows of its existence.

Chapter 2 - How Bitcoin Works

To understand how Bitcoin works, it is necessary to start with cryptography.

Cryptography protects private information by translating it into an unreadable text that cannot be deciphered without the proper decryption key. Bitcoin uses a cryptographic tool known as a hash function.

A hash function is a set of rules that transforms any size information into a uniform piece of data, the 'hash.'

A well-known example is the International Standard Book Number System (ISBN). This code uniquely identifies different books and is usually placed on the back cover. The ISBN transforms information, in this case, the specific edition of a particular book, into a standardized string of 13 numbers.

This, for instance, allows bookshops to check whether a particular edition of a specific book

is still available for purchase, among many other things. So, for example, the ISBN' hash function' of the first edition of "Harry Potter and the Philosopher's Stone" shows the value 9780439708180.

Two distinguishing features of hash functions are that they are easily computable, and the same input always gives the same output. Furthermore, it's impossible to go back to the information when starting from the production. Returning to the example mentioned above, any copy of the first edition of "Harry Potter and the Philosopher's Stone" will have 9780439708180 as its ISBN. However, there is no way to apply the same hash function to the value 9780439708180 and get "Harry Potter and the Philosopher's Stone" as a result. In simpler words, hash functions are one-way.

A third property shows that two inputs can't give the same output. To prove my point and continue our example, "Harry Potter and the Philosopher's Stone" is only associated with the ISBN 9780439708180; it's easy to see how having two or more ISBN codes

identifying the same book would be a logistical problem for a library.

Most hash functions are algorithms, or more simply, a set of rules that tell a computer how to convert an input into a string of characters. There are many different algorithms, but we are interested in Secure Hashing Algorithm 256, often abbreviated to the form SHA-256.

SHA-256 tells a computer to use a series of complex steps to turn any information into a string 256 characters long, consisting only of 1s and 0s. For example, the SHA-256 in the name "Billy" is:

1100100000110110100101011100111110011

To facilitate readability of the output, a hexadecimal system is used, which converts each set of four 1's and 0's into a single letter or number. The SHA-256 of the name "Billy" therefore looks like:

85eea4a0285dcb11cceb68f39df10d1aa132567

As you can see, this is already a much more streamlined and usable form compared to the previous one. However, for simplicity's sake, from now on, we will exclusively use the

hexadecimal system to show the results of hash functions.

The fourth property of hash functions, which SHA-256 also shares, is that a minor change in the input generates a significant difference in the output. The image below illustrates this concept well. As you can see, the slightest change in the use of capital letters in the word Bitcoin leads to totally different results.

SHA-256 is very useful because 256 digits, consisting of 1 and 0, give many possible combinations. Thus, we are talking about 2256 possible outputs, over 5 billion times the number of atoms in our galaxy. This allows SHA-256 to process a virtually infinite

amount of information.

But the question remains: how does Bitcoin fit into all this? It will soon become a lot clearer.

Bitcoin is nothing more than software that uses hash functions to create a form of digital money.

To understand how this happens, we need to step back and ask ourselves what digital money is. As we know, it's an electronic medium of exchange with many of the same properties as ordinary paper money: that means it's easy to transfer, difficult to counterfeit, and anonymous. Credit and debit cards and services like PayPal appear to be some digital money, but, unlike Bitcoin, there are always third parties involved: banks, credit card companies, and financial institutions.

On the other hand, cash is anonymous and easily transferred from one person to another; it requires no third-party intervention during transactions, and its value is known and shared by all. That being said, digital money

has a significant problem compared to cash. With cash, every single unit (such as dollar or pounds) can only be spent once. After payment has been made, the unit in question changes ownership. Therefore, its previous owner can no longer spend it. This may sound trivial, but it poses a big challenge for digital money: digital money could be pretty easy to counterfeit. Since a "digital payment" would consist of a series of 1's and 0's, one could duplicate that string of numbers and counterfeit the amount held by different accounts. If everyone could easily make copies of this "digital money," such a currency would quickly become worthless. This problem is known as the double-spending problem.

The only way to solve it seems to be to use a register that keeps track of how much digital money is held by different individuals at any time and through which all transactions are recorded. On the other hand, if a third party maintained this register, it would no longer be a digital transposition of cash, rather a transposition of credit. It would be, once

again, a situation where one has to put a certain degree of trust in a stranger.

Therefore, the real challenge for digital money lies in implementing a decentralized way to keep track of transactions and their balances.

Bitcoin solves this problem by making use of the hash mentioned above functions. It all seems to make more sense now, doesn't it?

A good thing to know about Bitcoin, when written with a capital 'B,' it refers to the technology as a whole. A lower case 'b' refers to the individual units of the system. In Bitcoin (with a capital 'B'), transactions are encrypted using the SHA-256 hash function.

The outputs of bitcoin transactions are collectively tracked by a decentralized network of computers communicating with each other over the internet, without a central entity. This type of cataloging is called a distributed ledger. Any network participant who wants a copy of the ledger can request and obtain one. Moreover, anyone can join the network by downloading the Bitcoin

software.

Unlike a centralized ledger, where only a trusted third party can add transactions to the ledger itself, a distributed one allows anyone to add transitions, admitting they follow a specific set of rules. In the following few pages, we will follow a bitcoin transaction from start to finish and see how it gets added to the Bitcoin ledger.

How transactions are added to the ledger

If Marie wanted to send a bitcoin to her friend James, she would have to message the Bitcoin network containing this information: "Marie sends a bitcoin to James." This transaction would be grouped up with other pending transactions; the group formed is known as a memory pool, often abbreviated to mempool. The transactions in the mempool are awaiting confirmation and can be recognized by all network users. By way of comparison, we can think of this stage as the

moment in a restaurant when the waiter has already taken the order. Still, the cook has not yet prepared the dish.

Any user can try to validate mempool transactions by grouping them into 'blocks.' Users who validate transactions are known as 'miners.' According to protocol rules, to validate a block of pending transactions, the miner must check their copy of the ledger, which includes all previous bitcoin transactions, to ensure that Marie has a bitcoin to send to James. They then do the same with any other transactions in that same block. To be added to the ledger, this block of transactions will be subjected to a hash function using SHA-256; this means that the 1's and 0's that make up the transaction "data" in the block produce a unique 256-digit number that will then be converted to a reduced form composed of 64 digits through the hexadecimal system.

In addition, the hash of the previous block is also included in the new block itself. By having this hash in each new block, a blockchain is created. Each block contains

the entire history of all previous transactions. This is possible because the SHA-256 function has an almost infinite number of outputs. Therefore each new block of transactions can have its hash. Since the hash of each block is calculated using the hash of the previous one, each new block is related to all previous ones, including their transactions. A small change to any one of them, such as adding a fraudulent transaction, would completely change the hash of each subsequent block, and miners would notice the error and immediately reject the block containing the fraudulent transaction.

This is essential, as transactions can only be added to the blockchain in new blocks and can never be changed or deleted later. Consequently, to ensure that Bitcoin's blockchain is valid, miners do not need to examine every previous block, only the hash of the most recent block, as it's all connected. This is important because once a transaction is added to the blockchain, it is considered part of the network and is publicly visible to

anyone. To see a transaction on the Bitcoin blockchain, we use a service like Blockchain Explorer (www.blockchain.com/explorer) and search for the hash of the transaction we are interested in.

At this point, the most attentive reader will be wondering, "but how does one decide who validates the transactions of any given block?".

According to Bitcoin's protocol, only blocks whose hashes begin with a certain number of 0s can be added to the blockchain. The idea is to create a competition between miners to determine who adds the next block of transactions. Not to be forgotten, SHA-256 hash outputs are unpredictable, so changing a single character of the input data will drastically change the outcome. This means that for the hash output of a transaction block to start with a certain number of 0's, miners must add an arbitrary number to the block, known as a nonce, and see the resulting hash. Since any SHA-256 output is unpredictable, the only way is to test different nonces as

quickly as possible arbitrarily.

As of April 2018, Bitcoin requires that transaction blocks only be added to the blockchain when the block hash starts with 73 0s. Unfortunately, this means that on average, miners have to test about 1.9 x 1022 hashes before finding a winning hash, with a probability of actually seeing it equal to 0.0000000000000001%.

The chances of a miner finding the correct nonce are proportional to the computing power they use. However, no miner can know if and when they will find the correct answer. This is crucial. Suppose a miner could guarantee to validate a specific block. In that case, the latter could include fraudulent transactions and irreparably damage the network. This is the essence of Bitcoin's distributed ledger. Instead of having a single entity, like a bank, validating and keeping track of transactions, many people compete to validate each block of transactions. The validation process, i.e., solving the cryptographic hash function, takes time and computing power. This process is called

Proof of Work and is often abbreviated to POW.

Bitcoin's difficulty is adjusted every 2,016 blocks to ensure that a block is found roughly every ten minutes. This is an arbitrary amount of time that allows the protocol to maintain a predictable DCAe. It also minimizes the risk of two miners validating two different blocks at the same time.

Miners' compensation

If block validation is so complex and expensive, why would anyone bother with it? The answer is quite simple. For each validated transaction block, the protocol allows the miner to add a particular additional transaction. This transaction states that the Bitcoin protocol must pay a certain amount to the miner who validated the block itself. This transaction is also known as “coinbase”.

The mining premium is the only way new bitcoins are put into circulation. The Bitcoin protocol has limited the number of circulating

bitcoins to 21 million. Therefore, the miner can only collect the reward if other miners accept their blocks. Like any other transaction, the coinbase transaction will only be accepted when agreed upon by all. This will only happen if all other transactions in the block are valid and a winning hash is found. Miners will continue to provide this service as long as the reward they receive is greater than the costs of validating the blocks. These costs include electricity and the computers needed for mining.

The more miners try to validate blocks and get their rewards, the greater the competition. The greater the competition, the more "random" the validation process. The more 'random' the validation process, the more secure it is. Randomness is at the heart of what makes a trust-less distributed ledger possible and safe. From all this, we can see that Bitcoin is a circular ecosystem in which each part "feeds" the next.

People can only exchange bitcoin securely with each other because the validation process is widely distributed, which is only

possible. After all, many miners are performing the validation that only operates because they receive rewards in bitcoin, which only has value because people can exchange it and convert it into euros or dollars. This balance of interests, competition, and incentives is perhaps the most ingenious concept behind bitcoin.

Halving

Just as the ECB has policies on when to inject new money into the European economy, Bitcoin's protocol has some rules on how bitcoin units are added to the ecosystem and how hard it is for miners to earn them. The reward in bitcoin for successfully validating a block is halved every 210,000 blocks or about every four years. In 2009, the reward was 50 bitcoins per validated block. In 2012, the first "halving," and the reward was reduced to 25 bitcoins. In 2016 it was down to 12.5, and in 2020 to 6.25. Doing a few calculations, this

geometric progression means that by 2140 all bitcoins will have been distributed. On the Coin Market Cap website, you can keep track of the time remaining until the next halving (coinmarketcap.com/it/halving/bitcoin).

In addition to the premium for block, miners collect transaction fees. Users pay these to incentivize miners to include their transactions in the first available block. When all bitcoins are distributed, these transaction fees will ensure that miners still have an incentive to validate blocks. The fees are not related to the amount of bitcoin in the transaction but are based on the file size of the transaction and market supply and demand.

Private Keys and Public Keys

Another essential part of Bitcoin's protocol that cryptography helps manage is authenticity.

When Marie starts a transaction stating she is transferring a bitcoin to James, how does the

recipient know it's him? And how does James know where the bitcoin in question is coming from? Cryptography gives us the answers. Every user on the network has a string of characters that acts similarly to a public "email address" for bitcoin transactions, also known as a bitcoin address. If you want to send bitcoin to someone, you need to know their bitcoin address. Just like email addresses, anyone can create as many bitcoin addresses as they please.

A Bitcoin address is derived from a public key, which is derived from a private key, the latter being an arbitrary string of 256 1's and 0's that should be kept secret, as it acts like a password for one address. The aforementioned public key is a number derived from the private key through an irreversible complex multiplication called the elliptic curve multiplication. This process aims to create a specific relationship between the public key and the private key. Firstly, this relationship is one-way: you cannot obtain the associated private key even if you know the public key. Furthermore, if you use

a special algorithm involving the cryptographic process known as the "Elliptic Curve Digital Signature Algorithm (ECDSA)" to combine a bitcoin transaction with your private key, you will get another number, the so-called signature. Thus, anyone who has the public key and the transaction's hash can look at the signature and see if it was indeed the correct private key that created it, even without knowledge of it. This is extremely important as it allows signatures to be used to authenticate transactions.

It is therefore clear that it is essential to keep one private key secret. If someone were to find out about it, they could use it to sign transactions posing as someone else, potentially stealing all their bitcoins.

So, when Marie sends a bitcoin to James, she includes three critical elements in the transaction:

- The signature
- The transaction
- His public key

This transaction is sent to James's address, which is derived from his public key. A Bitcoin address allows a certain degree of anonymity to be maintained. However, one must remember that all transactions are visible on the network. This is why it is essential to have the option not to include one personal detail in a transaction. Otherwise, the secrecy of this impersonal and "unsupervised" (by third parties) transaction is lost.

In the picture, you can see an example of a bitcoin transaction. As you can see, the actual names of the holders of the addresses involved in the transaction never appear. At the bottom, you can also see the "fees" paid, i.e., the commissions. As mentioned, these will be handed to the miner who validates the block in which this transaction is present.

The next chapter will talk about the best ways to store and remember your public and private keys.

To recap

- Bitcoin (with a capital 'B') denotes the protocol, while bitcoin (with a small 'b') denotes the coins themselves.

- Bitcoin transactions are encrypted using the SHA-256 hash function.
- Bitcoin transactions are processed in groups, also known as blocks.
- Miners validate blocks through a consensus mechanism called Proof of Work.
- Miners are paid in bitcoin to validate blocks.
- Miners' rewards are halved for every 210,000 blocks in a process called halving.

Chapter 3 – Wallets

In its simplest form, a wallet is a method of storing a private key. Some wallets are online and password-protected, while others consist of hardware and require both the password and the possession of the physical device to access said private key. A simpler alternative consists in writing your private key on a piece of paper and never sharing it with anyone. You have to be careful not to lose or forget it because, as we've seen, there is no way to generate it from a public key. Losing your private key, therefore, means you lose access to your bitcoins.

Generally, wallets can generate private keys, public keys, and bitcoin addresses, allowing the user to interface with the Bitcoin network, so they can send and receive bitcoins to and from various users and, when they choose to, view their balance in real-time. But, of course, like any storage, there are trade-offs between security and accessibility.

Online wallets that allow you to send and receive bitcoins quickly are less secure; Simultaneously, they can be accessed anywhere. The websites that host them may be vulnerable to hacking. To draw a parallel, one could think of online wallets as a physical wallets: you don't usually keep a lot of money in your wallet because there is a chance it could be stolen at any time. To give an example, one of the best online wallets is Exodus (exodus.com).

In contrast, a hardware wallet is a physical storage device. Hardware wallets may be less user-friendly for everyday use but are more secure since no one without the physical hardware can access the private keys stored inside. By analogy, they are similar to a safe in which real valuables are kept safe by trading off easy accessibility. Two of the best hardware wallets are Ledger (ledger.com) and Trezor (trezor.io).

In any case, it is essential to remember that bitcoins are not 'stored' in wallets in any way. Bitcoins are represented on the blockchain as transactions from one address to another, and wallets are merely a way of showing the balance of transactions to and from your address. Bitcoins are therefore not in wallets since these contain nothing more than the credentials to access the coins themselves.

For security reasons, you should only purchase hardware wallets or access online wallets from official sites.

To recap

- A wallet is a method of storing a private key.
- Losing your private key means you completely lose access to your bitcoins.
- Online wallets make it easier to send and receive bitcoins but are less secure.
- Hardware wallets are less user-friendly for everyday use but much more secure.

- The bitcoins themselves are not in the wallets. Only the credentials to access them are kept in the wallets.

Chapter 4 - Forks

At this point, a doubt may arise. If there is no central entity, who decides the rules the Bitcoin protocol must follow? And most importantly, is it possible to make changes? In this chapter, we will answer these questions.

Initially, the code for the Bitcoin protocol was written by someone who goes by the pseudonym Satoshi Nakamoto and, with him, a small group of developers. Among enthusiasts who have been following its evolution for a long time, the first version of the software is known as Bitcoin Core. However, none of the developers own the technology behind Bitcoin Core. In the same way, no one owns the technology behind the internet. As you will be aware by now, the Bitcoin network is distributed and therefore owned by everyone. Several developers are working to improve the Bitcoin Core software. Still, they cannot freely introduce changes to the protocol as network

participants can use their version of the software. Similarly, users cannot simply change their software to give themselves an advantage over the rest of the network, as the new protocol would be incompatible with all computers still using the old software.

From time to time, a group of miners or users may agree to update or modify the software to improve security or add functionality to the protocol. Anyone can suggest changes to the software, and these proposals are known as BIP, which is short for Bitcoin Improvement Proposals. Improvements to the Bitcoin protocol can be made in two ways: through soft forks and hard forks.

Soft Forks

A soft fork is a modification to Bitcoin's protocol that may cancel previously valid blocks and transactions. However, blocks valid under the new rules would still be valid under the old rules. Thus, a soft fork can be thought of as a tightening of the rules.

Imagine a "soft fork" styled change in rules concerning the dress code in the hypothetical workplace. For example, if the dress code requires men to wear a shirt, a soft fork could add a tie. Wearing a tie was never against the previous dress code rules, so it's technically compliant with the old rules. However, it becomes an imposition within the new dress code in juxtaposition to it only being an option beforehand. At this point, wearing a tie complies with both the old and new rules, but not doing so violates the current rules.

Returning to the world of Bitcoin, an example of a soft fork is allowing Bitcoin to include more transactions in blocks. According to Bitcoin Core, miners can validate around 2,500 transactions per block. This limit is a result of the single block file size, which is set to one megabyte. This is quite limited and equates to about four transactions per second. By contrast, the Visa circuit can process more than 2,000 transactions per second.

Consequently, some developers have proposed BIP141, known as SegWit or Segregated Witness. SegWit separates

transactions from their signatures. With this new structure, digital signatures no longer count towards the one-megabyte block size limit, allowing for more transactions per block and thus higher transaction speeds. Of course, blocks implementing SegWit were already valid under Bitcoin's original protocol rules. Still, after most miners adopted BIP141, SegWit blocks became a prerequisite for adding valid blocks to the blockchain.

The hard fork

Let us now take a look at the same block size limit problem but propose a different solution. BIP91 suggests increasing the block size to 8 megabytes. This would allow tens of thousands more transactions per block. If BIP91 is approved, future blocks would have a block size of 8 megabytes, and the old 1-megabyte blocks would no longer be valid. However, the 8-megabyte blocks would not be valid under Bitcoin's old protocol rules because the blocks had to be strictly one megabyte. This would create an

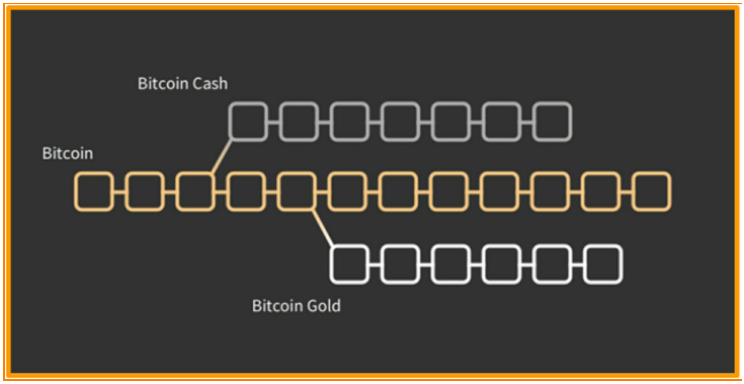
incompatibility between the two blockchains. When a change such as BIP91 is implemented, a hard fork occurs. Blocks from the old chain are incompatible with the new chain and vice versa. Assuming that miners support both the old and the new protocol, there will be two different blockchains and cryptocurrencies; one with the old rules and one with the new.

BIP91 was implemented on August 1, 2017, and kicked off the Bitcoin Cash blockchain. Bitcoin Cash follows all the rules of Bitcoin's protocol, except that the block size is 8 megabytes. Thus, for every bitcoin a user-owned at the time of the fork, they received one "bitcoin cash." At the time of the fork, Bitcoin Cash had an identical blockchain to Bitcoin. Only after the implementation of the upgrade did the two chains go their separate ways.

The value of a bitcoin cash does not necessarily equal that of a bitcoin since the fluctuating market always decides the price.

The image below illustrates this well by graphically showing the forks of Bitcoin Cash

and another branch that was later added known as Bitcoin Gold.



In typical human fashion, between 2014 and 2018, many developers saw hard forks as a chance to generate money "out of thin air." This led to a significant number of hard forks, which gradually generated less and less interest. Listed below are the most important hard forks in Bitcoin's history:

- Bitcoin XT (BIP64, June 2014)
- Bitcoin Classic (BIP109, November 2016)
- Bitcoin Cash (BIP91, August 2017)
- Bitcoin Gold (October 2017)
- Bitcoin SV (November 2018)

To recap

- The code for the Bitcoin protocol was written by the pseudonym, Satoshi Nakamoto. His identity is unknown.
- Anyone can propose an improvement to Bitcoin's protocol.
- A soft fork is a change to the Bitcoin protocol that does not create a second blockchain.
- A hard fork is a modification to the Bitcoin protocol that generates a second blockchain.

Chapter 5 - Buying and Selling Bitcoin

There is still one step missing to fully understand how Bitcoin works: how does one acquire it without being a miner?

The primary way most people get their hands on it is by buying bitcoin on an exchange site. These sites allow you to exchange regular money, such as euros and dollars, for bitcoin or other cryptocurrencies. Internationally, the two best-known exchanges are Coinbase (coinbase.com), which was listed on the NYSE at the beginning of 2021, and Binance (binance.com). Both of these platforms offer the possibility of depositing money either by bank transfer or by debit card. The purchase procedure is straightforward and will not be described in detail in this book, as the aspect of "where to click to do this or that" can change at any time. Exchanges also allow you

to sell bitcoins and other cryptocurrencies by converting them into an international currency and then withdrawing it from your bank account.

Suppose you'd prefer to rely on an European solution. In that case, TheRockTrading (therocktrading.com) and Young (youngplatform.com) are the most widely used services within our nation.

Whichever platform you decide to use, the recommendation is always to move your bitcoins to your wallet and not leave them on the exchange. After all, as the Americans say, "not your keys, not your bitcoin." A striking example of this concept was the 2014

hacking attack on the Mt.Gox exchange, during which 30% of all bitcoins in circulation were stolen: the total sum stolen was worth hundreds of millions of dollars.

To recap

- Bitcoins can be bought on an exchange site.
- You should always move your bitcoins to your wallet for security reasons and not leave them on the exchange.

Chapter 6 – Putting Everything Together

Now that we understand all the puzzle pieces let's take a step back and follow a bitcoin transaction from start to finish. In this case, let's turn back to the example of Marie sending a bitcoin to James.

1. Marie sends the message "Marie sends a bitcoin to James" to the network. This message includes Marie's public key, the transaction value, and her signature, which we remember is a combination of the hash of the transaction and her private key.
2. Marie's transaction ends up in the mempool with other pending transactions, waiting to be added to the blockchain by a miner.
3. A miner groups some of these transactions into a block, checking

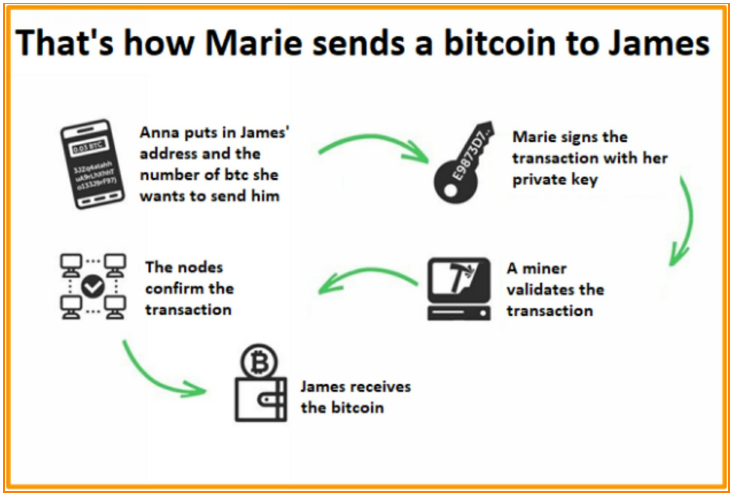
that the signatures are valid.

4. Miners repeatedly hash the transaction blocks, along with the hash of the previous block and a random nonce. Miners change the nonce randomly on each attempt until their block returns a winning output that starts with a precise number of 0s.
5. The first miner to hash a winning output gets the right to validate the block. Within the block, the miner includes a particular transaction called a coinbase. A reward in bitcoin is given, according to the rule in place when the block is validated. If the block were validated in September 2021, the coinbase would be 6.25 bitcoins in value. Along with the coinbase, the miner also receives all transaction fees contained in the block it has validated.
6. The block is added to the blockchain after the nodes have confirmed the validity of the block. As each block

includes the previous block's hash, the last block contains the proof of every transaction that ever took place.

7. At this point, the bitcoin sent by Marie is available in James's wallet, who can send it to another person, store it or convert it into money by sending it to the address given in his account on the exchange site chosen to use.

The image below illustrates this process graphically.


That's how Marie sends a bitcoin to James
Anna puts in James' address and the number of btc she wants to send him
Marie signs the transaction with her private key
A miner validates the transaction
The nodes confirm the transaction
James receives the bitcoin

Chapter 7 - The Blockchain

Since the creation of Bitcoin, there has been considerable interest in understanding how the underlying technology, ergo the blockchain, can be helpful in other contexts.

Bitcoin was the first distributed ledger system that did not require a centralized server or organization. Later, other cryptocurrencies emerged with new properties and characteristics. For example, Monero and Zcash seek to add an extra layer of privacy by obscuring transaction data. Litecoin, on the other hand, has tried to increase the block validation time to 2.5 minutes, allowing for faster transactions. To date, there are 11,000 different cryptocurrencies, as can be seen on CoinMarketCap (coinmarketcap.com), the reference site for those who want to study the economic dynamics of various projects.

Proof-of-Work, Bitcoin's consensus mechanism, is very effective in creating a

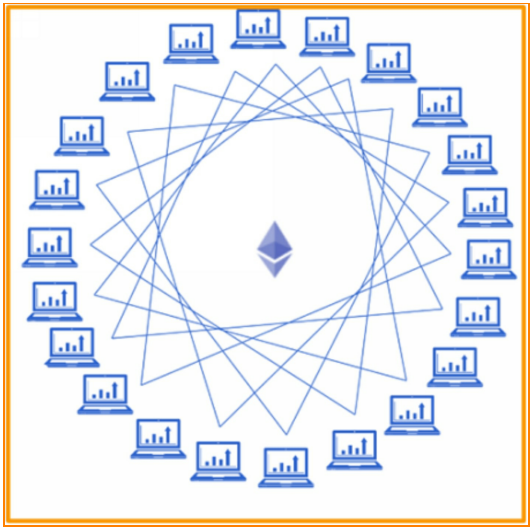
random and decentralized mining process. Still, it also requires a lot of electricity. The hashing process requires electricity and, with the total hash rate of the Bitcoin network at about 23 million billion hashes per second, it has been estimated that each bitcoin transaction requires about 886-kilowatt hours of electricity. This is equal to the daily electricity consumption of 30 American households.

Since this power consumption has no other function than to support Bitcoin transactions, some alternatives to Proof-of-Work have been suggested. One idea is to use a mechanism known as Proof-of-Useful-Work,

which uses the computational power of mining to solve a concrete problem and advance science while working on a transaction. For example, one could use Bitcoin mining to find large prime numbers.

Another more practical solution to reduce power consumption is to use a consensus mechanism known as Proof-of-Stake (abbreviated to POS). In this case, the person validating a block would be identified through a random selection based on the user's amount of value blocked (also referred to as "staked").

Bitcoin provided us with the mold we can use to build a platform and infrastructure to trade digital currencies over the Internet without needing a trusted intermediary. Still, the most significant innovation since then has to be sought elsewhere. Specifically, in Ethereum, the second most capitalized cryptocurrency developed in 2015. In short, Ethereum is a decentralized computer that allows you to build other decentralized applications. Don't worry; we will discuss Ethereum in more detail in the coming chapters.



In this case, we must continue to analyze what makes sense to decentralize and what does not. Still, some contexts that can benefit from decentralization include:

- Financial markets
- Databases of sensitive data
- Transport networks
- Intellectual property rights

Some businesses are also interested in using blockchain solutions, building their private blockchains to manage workflow, or offering services to other companies. For example, the

first private blockchains have already been used to keep track of bank transactions and reduce the time it takes to credit transfers. In addition, market leaders from every interested sector are testing profusely to create solutions that can guarantee data integrity and validity.

To recap

- Proof of Work is not the only consensus mechanism.
- Proof of Work is very energy-intensive.
- Proof of Stake aims to solve the critical issues presented by the Proof of Work system but has so far only been implemented on very few blockchains.

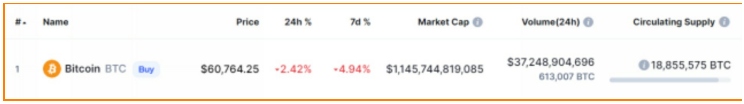
PART 2 - THE CRYPTOCURRENC ECONOMY

Chapter 8 - The Economics of Bitcoin

Before talking about other cryptocurrencies, it is necessary to establish some parameters to define the pricing and value of different projects. After all, with over 11,000 cryptocurrencies, it's easy to get lost and not understand how to continue your study after analyzing Bitcoin.

This chapter intends to define some key concepts to assess the seriousness and reliability of a blockchain project.

By visiting CoinMarketCap (coinmarketcap.com), we notice that each cryptocurrency has an assigned value. We can analyze Bitcoin's case best since it's the one whose technological basis is now known.



#▪	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
1	Bitcoin BTC Buy	$60,764.25	-2.42%	-4.94%	$1,145,744,819,085	$37,248,904,696 613,007 BTC	18,855,575 BTC

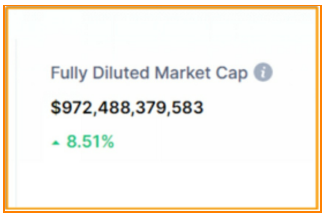
The first five columns are easy to understand. First, the number (in this case, number 1)

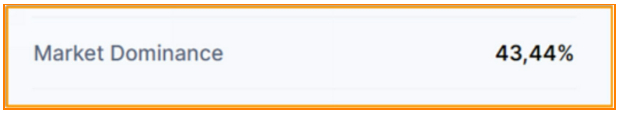
indicates its ranking: we can see that, as previously mentioned, Bitcoin is the most capitalized cryptocurrency. Next in the chart is the name, the ticker abbreviation (BTC), followed by the current market pricing and the change in price in percentage over the last 24 hours and the last seven days.

The item "Market cap" refers to the total capitalization. This value is derived by multiplying the price of a single Bitcoin (in the image 60,764.25 dollar) by the total circulating amount (in the image 18,855,575). Thus, capitalization indicates how much money is inside the Bitcoin protocol and identifies the total value.

This is followed by "Volume (24h)", which indicates the total value in dollar of transactions that have taken place on the Bitcoin network in the last twenty-four hours. Finally, the last column shows how many Bitcoins are in circulation right now. The completion bar below the numerical value graphically shows how many Bitcoins are in circulation compared to the total supply, which we know is 21 million.

If we then click on the words "Bitcoin," we enter the cryptocurrency's main page. Here we can see other interesting data, such as the "Fully Diluted Market Cap" and "Market Dominance."





The "Fully Diluted Market Cap" indicates the market capitalization of all available coins was already in circulation. This value is the market price multiplied by the maximum number of coins, in this case, 21 million. "Market Dominance," on the other hand, is a percentage that expresses how much Bitcoin's capitalization weighs on the total capitalization of the entire cryptocurrency market. The total capitalization is the sum of the different capitalizations. The total market capitalization value can be found atop the screen, where the total value of all

transactions in the cryptocurrency market in the last 24 hours also appears.

CoinMarketCap is a crucial tool, as it allows you to identify the “size” of any given cryptocurrency at a glance. It tends to be the case that all cryptocurrencies that are not in the top 100 are not worth studying or buying. Of course, there are always exceptions to this rule; however, a systematic approach to studying this sector must have some parameters on which to base it.

To recap

- Price does not say much about the market's interest in a cryptocurrency.
- Capitalization allows you to understand how much money there is in any given protocol.
- Capitalization is calculated by multiplying the number of coins by the price of a single currency.

Chapter 9 - The Problem With Capitalization

As we have seen, capitalization indicates how much money there is in any given cryptocurrency and how this number depends on both the pricing and the total amount of circulating coins. This means that a cryptocurrency with a high price does not necessarily have a high capitalization. For example, Yearn Finance, despite having a cost of around 35,000 dollar, does not have even a tenth of the capitalization of Bitcoin.

The reason behind such a high price is the maximum amount of coins available. In this case, the chart shows only 36,638 YFIs in circulation, compared to 21 million Bitcoins. Therefore, to have the same capitalization as Bitcoin, each Yearn Finance protocol coin would be worth around 20 million.

That being said, often, those who first

approach the world of cryptocurrencies are fooled by the exact opposite; they tend to think that coins that cost less are more likely to grow. After all, if Bitcoin has reached 60,000 dollar, any cryptocurrency would be worth a dollar, right? Wrong. The example of Shiba Inu (yes, there is a cryptocurrency named after a breed of dog) is apt.

As can be seen, the price of a SHIB is not even close to one cent. However, this figure has to be weighed against the number of coins available. In this case, we are talking about a circulation about 19 million times larger than that of Bitcoin. This means that for every Bitcoin in circulation, there are 19 million SHIBs. Now it is obvious why the price of a single SHIB is so low. If, absurdly, a SHIB were to reach the price of even just one dollar, that cryptocurrency would be worth ten times more than the S&P 500 (the index of the 500 most capitalized companies in the United States).

As you can see, the pricing of cryptocurrency tells us little or nothing about it. It is, in fact,

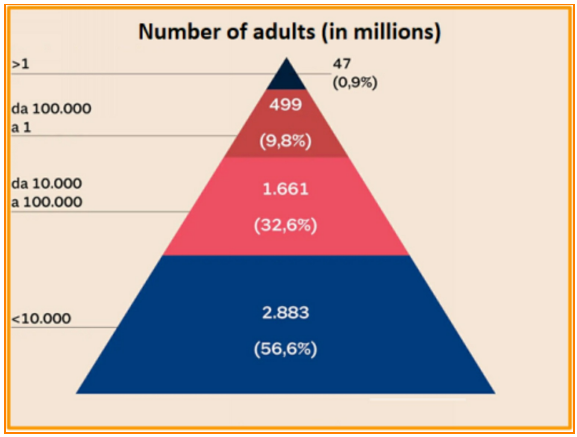
a figure that must be weighed against the capitalization of both the individual cryptocurrency and the entire market.

To recap

- Some cryptocurrencies deliberately have a high number of coins to give the impression of being cheap.
- Capitalization is the only data that can tell how much economic interest there is in a project.

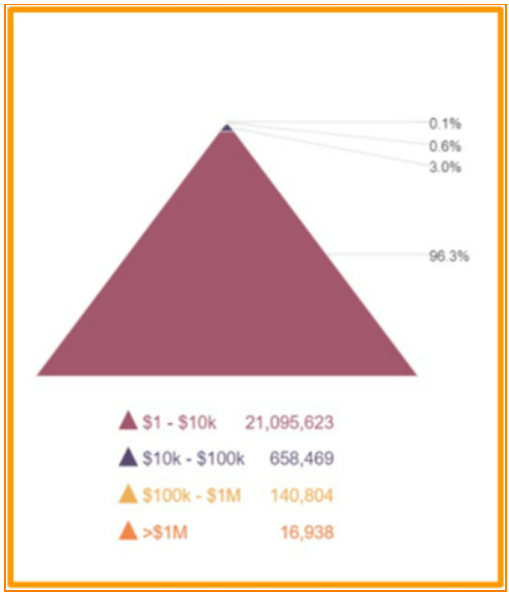
Chapter 10 – Wealth Distribution

Capitalization and pricing indicate how much money there is inside a blockchain protocol and, consequently, of users' interest in holding and using that specific cryptocurrency. However, a further question must be asked to understand the economics of a currency even better: how is the wealth of that protocol distributed? This is because any instrument used to hold or exchange value is not evenly distributed. A case in point is the US dollar, as can be seen in the image below.



Most of its value is controlled by a small part of the population. As you move down to the pyramid's base, the number of individuals increases while the purchasing power decreases.

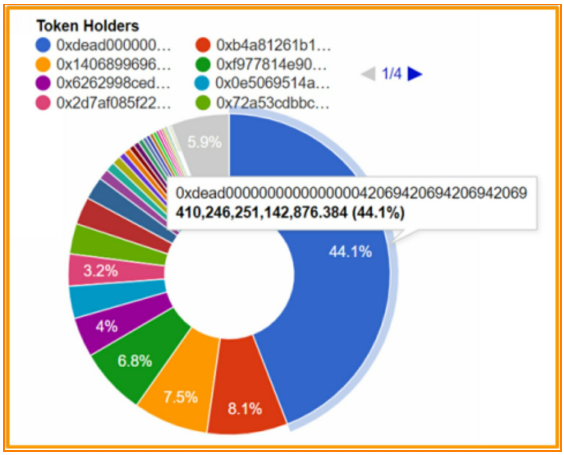
Since all cryptocurrencies in the top 100 have a public blockchain, studying this distribution for each project is possible. As an illustration, let us see how wealth is distributed in the Bitcoin protocol. The following image is symbolic.



Most of the value is held by the largest share

of users. Bitcoin, in this sense, is much fairer than legal tender currencies. The reason for this distribution is the lack of institutional interest in cryptocurrency. Only since 2020 have large investors and financial institutions allocated some of their liquidity to Bitcoin. For the first eleven years of its history, Bitcoin was almost exclusively used by ordinary people, who were, therefore, able to accumulate a considerable part of the total circulating money.

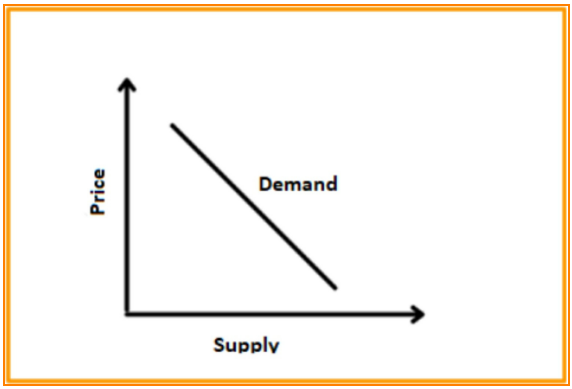
However, not all cryptocurrencies are distributed so equally; again, Shiba Inu is a perfect example.



Looking at the graph, it can be seen that a

single address holds 44.1% of the circulation. This means that the entire SHIB market is almost half controlled by one person. Moreover, this cryptocurrency was created in August 2020 and therefore counts on a relatively short life span. It is hard to believe that someone could have bought half of the total circulating amount in such a short period. On the contrary, it is easier to think that the developers arbitrarily assigned control over such a large amount of SHIB. The biggest threat for investors, in this case, is that at any given time, that single address could sell its coins, practically doubling the supply of SHIBs on the market and seriously decreasing the value of the currency. Since the price is always a match between supply and demand, doubling the supply without increasing demand leads to a drastic drop in price.

The picture clearly shows that as the quantity increases, the demand curve tends to steepen, leading to a drop in price.



Having to give a rough parameter, it's advisable to stay away from all cryptocurrencies where most of the wealth is concentrated in 10 or fewer addresses.

So, there are two parameters to consider when choosing a cryptocurrency to investigate:

- The project must be among the 100 most capitalized;
- The wealth of the protocol must not be concentrated primarily on 10 or fewer addresses.

All the cryptocurrencies that will be examined in the following chapters meet these two criteria.

To recap

- When analyzing a cryptocurrency, one must take into account how the coins are distributed.
- Coins with a high degree of concentration in a few addresses can be a risky investment.
- Projects that are in the top 100 by capitalization are the most solid ones.

PART 3 - ALTCOINS

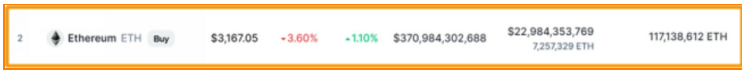
Chapter 11 – Ethereum

Cryptocurrencies outside Bitcoin are often called 'altcoins,' terms that will often be used in this book to generalize this category. However, it should not be assumed that these are projects actively trying to compete with Bitcoin. For the most part, altcoins serve different purposes other than just being a digital form of cash.

The altcoin from which we should start is certainly Ethereum; we made this choice for two reasons:

- It is the second-largest capitalized cryptocurrency;
- It allows the existence of most of the other blockchain projects.

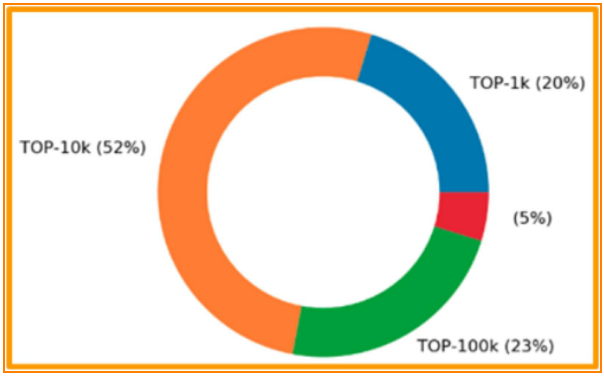
We start by examining the economic data to confirm that it meets the two parameters set out above.



CoinMarketCap shows that indeed Ethereum occupies second place in the ranking by capitalization. In addition, the more observant reader will have noticed that below the number of circulating coins, there is no progress bar as there was for Bitcoin. This is because Ethereum does not have a maximum amount of ETH placed on the market.

The distribution of wealth in the Ethereum protocol also respects our parameter, as shown in the graph below. CoinMarketCap shows that indeed Ethereum occupies second place in the ranking by capitalization. In addition, the more observant reader will have noticed that below the number of circulating coins, there is no progress bar as there was for Bitcoin. This is because Ethereum does not have a maximum amount of ETH placed on the market.

The distribution of wealth in the Ethereum protocol also respects our parameter, as shown in the graph below.



History of Ethereum

Ethereum was conceived in late 2013 by Vitalik Buterin, programmer and founder of the Bitcoin Magazine blog. Ethereum's goal, as written in the white paper, is to enable the construction of decentralized applications. Vitalik argues that the blockchain can be used to create a decentralized form of money and build an entire financial system that can function without a central authority. This requires a much more complex technological infrastructure than the one Bitcoin works with: this is where Vitalik's computer skills came in very handy.

The idea proposed in 2013 was then made

official in 2014 at the Miami Bitcoin Conference, when backers Gavin Wood, Charles Hoskinson, and Anthony Di Iorio began developing the project alongside Vitalik Buterin himself. Over the years, several established personalities have contributed to the construction of what is now Ethereum. Famous names in the industry include Joseph Lubin and Jeffrey Wilcke, who, by contributing, is remembered today for creating the world's most crucial altcoin.

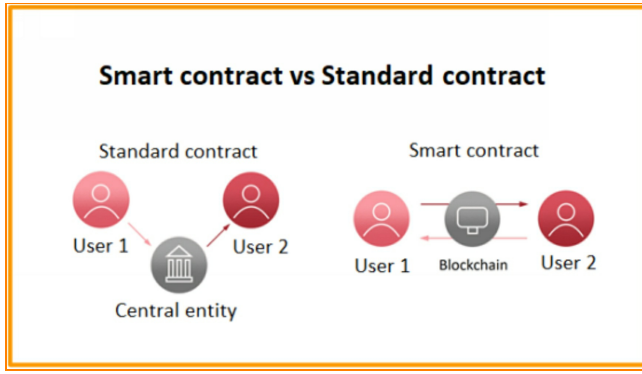
How Ethereum works

Ethereum is a decentralized network based on blockchain technology. This cryptocurrency differs from all others because it was the first to introduce the concept of smart contracts to the blockchain itself.

Smart contracts are programs written directly onto the blockchain, activated autonomously when specific conditions are met. As an example, let's assume that Marie and James have a rental contract. Usually, there would be a central intermediary, the bank. Every month James must pay rent to maintain the

possibility to live in Marie's house. However, if James decides not to make the payment, he is not immediately prevented from entering the house.

On the contrary, as is well known, American justice would take several months to take its course. A smart contract solves this problem at the root. For example, one could replace the lock with an electronic key and program a smart contract that allows the door to be opened only if payment has been made on time. The beauty of such a solution is that neither Marie nor James have to trust a central intermediary to enforce the rules. Suppose the blockchain does not record the rent payment transaction by the deadline. In that case, the smart contract is activated and prevents access. The following image illustrates this concept.



On the Ethereum blockchain, smart contracts have a public address. As a result, everyone can see this address and interact with it if they wish. Furthermore, it is possible to create smart contracts that interact based on what events occur. All smart contracts on Ethereum are written using the "Solidity" programming language and are initialized by the Ethereum Virtual Machine, often abbreviated to EVM.

One mustn't forget that being a blockchain, the smart contract that governs James and Marie's rent is not regulated by a single computer but by the entire network, which at the same time must also keep tens of thousands of other smart contracts active. This process has a high cost that must be paid

to the miners to incentivize them to keep validating the blocks containing the aforementioned smart contracts. These fees are paid in Ether (ticker ETH). So, unlike BTC, ETH does not act as digital money but as a 'gas' to enable the programming and operation of the network. This is why Ethereum is thought of by many as "programmable money." ETH can be held on the Ledger and Trezor hardware wallets and several specific online wallets, the most famous of which is MetaMask (metamask.io).

Ethereum mining

On Ethereum, a miner validates a new block every 10-15 seconds, unlike the 10 minutes required by Bitcoin. Smart contract transactions are written on the blockchain and therefore require a payment fee; just reading the data of a smart contract does not involve a transaction and is, therefore, free of charge. This allows all users to study the smart

contract before actively interacting with it. In the example above, James and Marie can read the rental agreement for free as many times as they like before activating it. The commissions paid by users to use a smart contract are given to the miners and a premium of 2 ETH for validating a block. Usually, commissions are measured in Wei, the unit of which is approximately 1x10-18 ETH. As with Bitcoin, users will compete on commissions to have their transactions included in a block first. The cost of Ethereum's commissions can be kept under control via the "ETH Gas Station" service (ethgasstation.info).

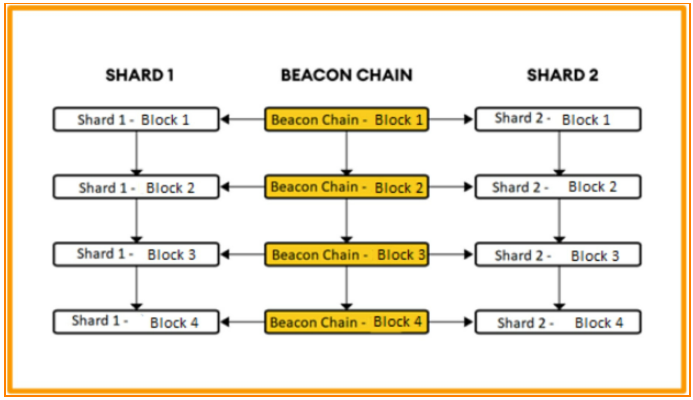
Ethereum has no halving events because it does not aim to store value in the network. ETH can be thought of as petrol for cars: its purpose is to keep the car running, not to be stored and used as a means to exchange goods with other car owners. Precisely for this reason, no maximum number of ETH can be put on the market.

ETH 2.0 and the transition to Proof of Stake

As mentioned in Chapter 7, Proof of Work is a relatively expensive consensus mechanism in power. It does not allow for colossal scalability, as the difficulty of mining increases as new miners are added. A massive blockchain like Ethereum needs a solution that can process blocks very quickly and increase that speed over time. This is why, for the last few years, the developers of Ethereum have been preparing a major update to the network. This update is known as Ethereum 2.0.

By implementing several updates, speed, efficiency, and scalability should be improved without sacrificing security and decentralization. The main differences between Ethereum and Ethereum 2.0 concern the use of Proof of Stake as a consensus mechanism and sharding and as a beacon chain. POS has already been explained in chapter 6. So let us instead take a look at the other two innovations.

Anyone wishing to access the Ethereum network must do so via a node. These nodes store a copy of the entire blockchain, which means that they have to download, calculate, store and process every transaction since the network began to exist. This is an expensive process. Sharding allows nodes to keep only a tiny part of the Ethereum blockchain. In other words, sharding enables the creation of small blockchains that run in parallel with the main blockchain, thereby increasing the network's transaction speed and overall caDCAity. These parallel blockchains are called "shards."


SHARD 1
BEACON CHAIN
SHARD 2
Shard 1 - Block 1
Beacon Chain - Block 1
Shard 2 - Block 1
Shard 1 - Block 2
Beacon Chain - Block 2
Shard 2 - Block 2
Shard 1 - Block 3
Beacon Chain - Block 3
Shard 2 - Block 3
Shard 1 - Block 4
Beacon Chain - Block 4
Shard 2 - Block 4

The transition to ETH 2.0 has been divided into phases and is expected to be completed between 2022 and 2023.

At this point, the question arises: which decentralized applications are being built on Ethereum? The answer is simple: most "cryptocurrencies" in the top 100 by capitalization are applications that run on Ethereum's blockchain. By analyzing some of these in the following chapters, it will be easy to see what applications we are talking about.

To recap

- The objective of Ethereum is to enable the construction of decentralized applications.
- Ethereum was the first cryptocurrency to use smart contracts.
- Smart contracts are programs written directly onto the blockchain, activated autonomously when specific conditions are met.
- Ethereum's smart contract programming language is Solidity.
- The ETH token is used to pay network fees.
- The EVM executes the codes on each

node of the network simultaneously.

- Anyone can build a decentralized application.
- Ethereum is still based on Proof of Work but is making the transition to Proof of Stake.

Chapter 12 - Tether and Stablecoins

Tether (tether.to - ticker USDT) is the fourth most capitalized cryptocurrency and the most widely used stablecoin globally. However, before talking about USDT, we need to take a step back and understand what stablecoins are and what role they play in this industry.

Stablecoins

Stablecoins are a form of digital currency designed to mimic the value of legal tender currencies, such as the dollar or the dollar. Their purpose is to allow users to transfer a predetermined amount of a particular value onto a blockchain that will remain constant over time. On the other hand, cryptocurrencies such as Bitcoin and Ethereum are notorious for their volatility. The fluctuation in their prices makes them

inconvenient to use for short-term transactions.

To better understand the concept, let's re-examine the example of the smart contract governing the rent between James and Marie. It is much more convenient for Marie to receive the payment in any stablecoin rather than in ETH or BTC, as their value could vary significantly over even one day. For example, if James had paid $1,000 of rent in ETH the morning of 18 May 2021, at the end of the day, Marie would only have a counter value of $730. This is why smart contracts and decentralized applications must have stablecoin as possible options for users to choose from.

The most popular type of stablecoin is directly collateralized at a 1:1 ratio by a legal tender currency. In this case, a central issuer holds a certain amount of legal tender, e.g., dollars or euros, and, in return, issues a virtual currency for each unit of value held. For example, the issuer may save one million dollars on a current account and give one million coins worth one dollar each. Users

can freely exchange these coins as they would with 'real' dollar then, at any time, redeem them for legal currencies. In this case, there is a high degree of counterparty risk that cannot be mitigated in any way: at the end of the day, the user must trust the issuer. At best, the company issuing stablecoins can try to be as transparent as possible through regular audits of its reserves.

Another category consists of stablecoins collateralized by other cryptocurrencies. In this case, users lock up a certain amount of cryptocurrency in a smart contract to receive the corresponding stablecoin in return. Subsequently, it will be sufficient for users to send stablecoins to the address listed for the smart contract to unlock their cryptocurrencies. As one can assume, this variety presents no need to trust a central entity, as a smart contract regulates everything. However, the volatility of the collateral can, from time to time, cause losses in value when collecting the blocked funds. Maker DAO is the best-known stablecoin collateralized by other cryptocurrencies.

Nevertheless, as can be seen from its capitalization, it is used very little.

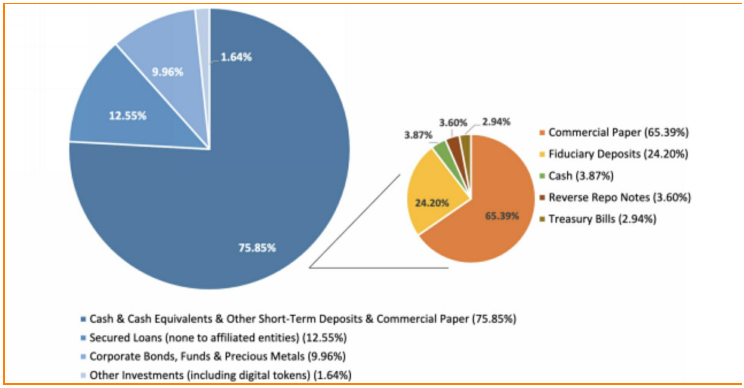
The last category we can analyze is algorithmic stablecoins. They are not collateralized by legal tender or other cryptocurrencies: their collateralization is handled entirely by algorithms and smart contracts that manage the number of tokens issued. Functionally, their monetary policy closely mirrors that used by central banks to manage legal tender currencies. Essentially, an algorithmic stablecoin system reduces the supply of the token if its value falls below the price of the currency it wishes to track. Conversely, suppose the cost exceeds the value of the legal tender. In that case, new tokens are put into circulation to reduce the value of the stablecoin. This is a practical application of matching supply and demand. Ampleforth is the best-known stablecoin collateralized by an algorithm, but there are very few users even then.

USDT

Tether is one of the stablecoins collateralized with legal tender. Unlike the other examples in this chapter, USDT is widely used and has held a prominent position in the cryptocurrency landscape for years. As can be seen, it is the fifth most capitalized project.

The smart contract that governs the operation of USDT was programmed by Tether Operations ltd and initially implemented on the Ethereum blockchain in 2014, following the programming standard known as ERC-20. Most decentralized applications on Ethereum are built relying on this standard, as it allows for excellent interoperability and ease of programming. In addition, ERC-20 tokens can be sent from and stored on any Ethereum address. This means that at the same address where a user keeps their ETH, they can hold their USDT. Especially in its early days, the price of USDT was a bit volatile, reaching as high as $1.2 for a few hours. However, since the beginning of 2019, this volatility has been

waning, probably thanks to a steady increase in its trading volume and the general progress of the cryptocurrency market. An interesting peculiarity is that the original paper stated that each USDT was collateralized by one dollar. However, with the passage of time and the increase of USD in circulation, Tether Operations ltd decided also to use other financial instruments as collateral to keep the value of the coin stable. The image below shows how the USDT reserves are distributed, allowing USDT to be effectively collateralized at a 1:1 ratio. The figures refer to 31 March 2021.



To recap

- Stablecoins are cryptocurrencies that

seek to maintain a stable value.

- Some stablecoins are collateralized by legal tender, others by cryptocurrencies and algorithms.
- USDT is the most heavily capitalized stablecoin.
- USDT is collateralized by both legal tender and other bankable assets.

Chapter 13 - Chainlink and Oracles

Oracles provide smart contracts with information that cannot be found within the blockchain. In other words, they serve as a bridge between the blockchain and the outside world. Although smart contracts cannot access external data, many contractual agreements must draw on information from the outside world. This is precisely where oracles come into play. They are crucial because they enlarge the sDCAe within which smart contracts can operate. Without oracles, smart contracts would have minimal use as they would only have access to data from their networks.

It is essential to point out that an oracle is not the source of the data itself but the entity that searches, verifies, and authenticates external data sources and transmits this information to the relevant blockchain. This data can include, among other things, information

about the price of a good or service, the completion of payment in the traditional banking system, or the outside temperature.

Recall the rental agreement between James and Marie. James might decide to pay Marie not by using USDT but by bank transfer. In this case, we would need an oracle to figure out when the bank transfer was made and update the smart contract, allowing James to enter the house. One solution would be to create an oracle that can read the transfer slips. It may seem not very easy to even imagine, but combining good programming with artificial intelligence is more straightforward than it looks.

There are many different types of oracles, which are usually grouped into two categories: centralized oracles and decentralized oracles.

Centralised oracles

A centralized oracle is controlled by a single entity and is the sole source of information

for a smart contract. Using only one source of data can be risky, as the effectiveness of the intelligent contract depends entirely on a single oracle. The main problem with centralized oracles is precisely the existence of a single point of failure, which makes contracts less resistant to vulnerabilities and external attacks. To be honest, centralized oracles are hardly ever used in the cryptocurrency industry today.

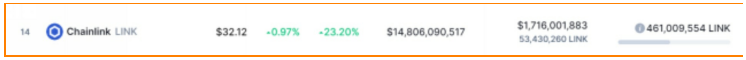
Decentralised oracles

Decentralized oracles increase the reliability of data provided to smart contracts by relying on multiple sources of information as opposed to one. In this case, the smart contract interrogates multiple oracles to determine the validity and accuracy of the data. However, this process also requires that smart contract users trust the oracles themselves less. Although the number of information sources cannot be unlimited, it is undoubtedly an advantage to have multiple resources to extrapolate the data relevant to

the specific smart contract. In addition to Chainlink, a very famous, albeit little-used, decentralized oracle is Band Protocol.

Chainlink

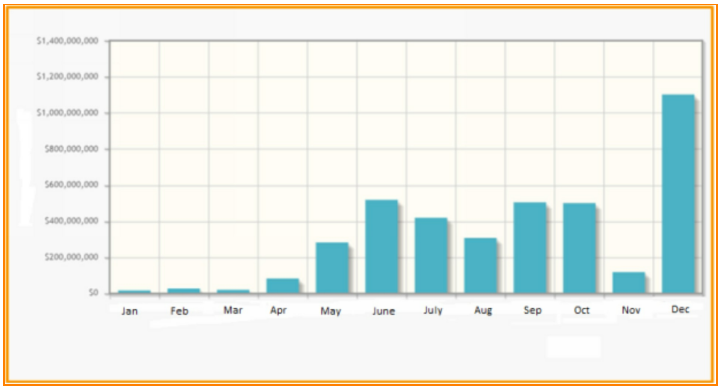
ChainLink (chain.link) is a decentralized oracle-based network that allows smart contracts to connect with entities external to the blockchain. These entities can include APIs, management systems, or other types of external data feeds. The LINK token follows the ERC-20 standard and is used to pay the network for the oracle service.



What makes this oracle so widely used is the process by which Chainlink validates data from multiple sources. Using a proprietary algorithm, Chainlink can determine which sources are reliable and which are not with relatively high accuracy. This dramatically increases the accuracy of the results and

protects smart contracts from possible hacker attacks.

Chainlink has a maximum supply of 1 billion LINK tokens. 35% of these were sold in 2017 through Initial Coin Offering, abbreviated as ICO. About 300 million LINKs remained in the hands of the company that founded the project (the SmartContractChainLink ltd). An ICO is when a company operating in the cryptocurrency sector decides to sell a portion of its project's tokens to the public to increase its capital. In 2017, this practice became very popular, leveraging the general euphoria of the market. However, as shown in the chart below, it peaked in December, right when Bitcoin hit its old all-time high at $19,000.



As you will be aware by now, being an ERC-20 token, LINK does not have its blockchain and can be held on any Ethereum address. The LINK token is used as a payment instrument for an oracle service; the smart contract gives the commission to the node chosen to provide the data. An interesting aspect is that Chainlink's proprietary algorithm provides more prominence to nodes with a high amount of LINK. It is assumed that they have already cooperated with many smart contracts in the past. This approach incentivizes node operators to continue accumulating LINKs. Those who invest speculatively in this cryptocurrency base their reasoning on this very point: since nodes are interested in accumulating, there will be low selling pressure, and the price of LINK can rise. This only works if there are a lot of smart contracts that use Chainlink as an oracle.

To recap

- Oracles serve as a bridge between the

blockchain and the outside world.

- There are centralized and decentralized oracles.
- Chainlink is a decentralized oracle.
- The LINK token is used for network governance and to be entitled to provide data to smart contracts.

Chapter 14 - Uniswap and Decentralised Finance (DeFi)

For years, centralized exchanges have been the backbone of the cryptocurrency market: they offer high trading volumes and ever-increasing liquidity. However, a parallel world is under construction, which leverages smart contracts to eliminate the need to trust an intermediary when exchanging cryptocurrencies.

Due to the inherent limitations of blockchain technology, it has been a challenge to build decentralized exchanges that can compete meaningfully with their centralized counterparts. One of the pioneers in this area has been Uniswap.

As a result of this innovation, Uniswap has become one of the most successful projects in the movement known as decentralized

finance.

Decentralised finance

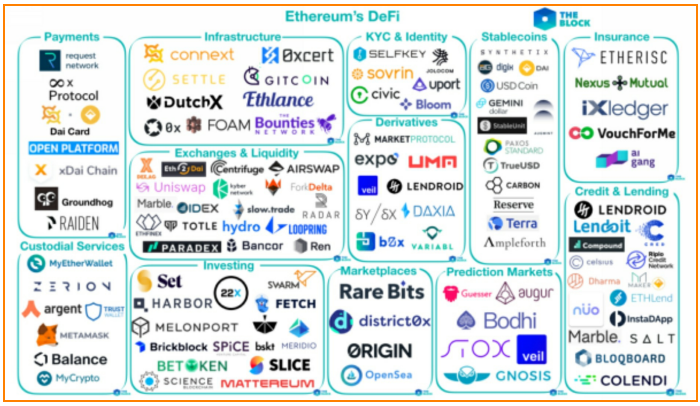
Centralized systems can increase the speed and limit the complexity of transactions by giving users less direct control over their money. Decentralized finance seeks to expand the use of blockchain from simple value transfer to more complex financial use cases. Indeed, value exchanges are not the only type of transaction or contract overseen by large corporations; financial applications such as loans, insurance, crowdfunding, derivatives, and betting are also under their control. Eliminating intermediaries from all types of economic transactions is one of the main advantages of decentralized finance.

The most popular types of decentralized finance applications include:

- Decentralized exchanges allow users to exchange cryptocurrencies by connecting directly with one another without having to trust an intermediary.

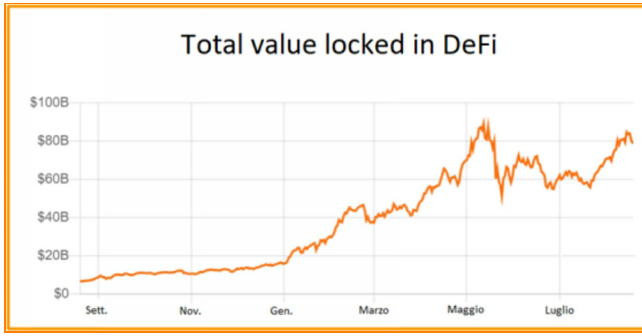
- Stablecoins, which, as we have seen, are a cryptocurrency that is collateralized by other assets and manage to maintain a stable value over time.
- Lending platforms that use smart contracts to replace banks in managing loans.
- Bitcoin wrappers allow bitcoin to be carried on the Ethereum network so that smart contracts can also be applied to the most capitalized cryptocurrency.
- Decentralized prediction markets allow people to bet on the outcome of future events, such as elections, without relying on a single source of information.

To date, most Ethereum applications deal with decentralized finance. However, as you can see, the amount of projects that make up this ecosystem is genuinely enormous.



Those who use decentralized finance applications aim to earn a return on their capital. Before the advent of this sector, it was not possible to receive “interest” in cryptocurrencies. This is undoubtedly a fascinating branch for investors who want to make the most profit from their positions.

This is precisely why decentralized finance is the sector for which most projects are being developed and in which most money flows. The following graph shows the immense growth that decentralized finance has seen over the last year.



Uniswap

Uniswap allows users to trade without intermediaries, with high degrees of decentralization and resistance to censorship. Although Hayden Adams created the protocol in 2018, the underlying technology behind its implementation was first described by Ethereum founder Vitalik Buterin.

Uniswap works with a protocol called Constant Product Market Maker. Automated market makers are smart contracts that hold vast reserves of cash with which traders can trade cryptocurrencies. These reserves are funded by users known as "liquidity providers." Anyone can become a liquidity

provider; to do so, one must deposit an equivalent value of two tokens. In return, fees from the exchanges are distributed to the liquidity providers according to their share of the total liquidity.

Liquidity providers create a market by depositing an equivalent value of two tokens. These can be either an ETH and an ERC-20 token or two ERC-20 tokens. Typically, liquidity reserves consist of a stablecoin such as USDT and an ERC-20 token, but this is not required. To better understand these concepts, an example is essential.

Let us consider the ETH/USDT liquidity reserve (the liquidity reserve is often called a pool). ETH will represent part x of the reserve and USDT part y. The Uniswap protocol takes these two quantities and multiplies them to calculate the total liquidity of the reserve: this value is denoted by k. The idea behind Uniswap is that k must remain constant over time for the service to perform well. This means that the total liquidity in reserve must be constant. Therefore, the formula to calculate the total liquidity in

reserve is:

$x * y = k$

So what happens when someone wants to make an exchange? Suppose Marie buys 1 ETH for 300 USDT using the ETH/USDT liquidity reserve. This way, the amount of USDT in the reserve increases while the number of ETH decreases. This leads to a rise in the price of ETH, although this may be barely noticeable given the size of the numbers.

Keeping in mind that k must remain constant since there are now fewer ETH in the cash reserve after the transaction, it is clear that this party decreases, the other must increase. Moreover, since physically, there cannot be more ETH or USDT than those paid into the reserve, this decrease is balanced by increasing the price. Thus, ultimately, Marie's price for ETH is based on how much her transaction has shifted the relationship between x and y.

It should be noted that this model does not follow a linear progression. The larger the

buy or sell order, the more significant the change in the ratio between x and y will be. This means that larger orders become exponentially more expensive than smaller orders.

Interesting to point out is the fact that out of this whole process, Uniswap does not earn a single penny. All commissions go to the liquidity providers, and none of the developers receive anything from the transactions on the protocol.

Currently, the transaction fee paid to liquidity providers is 0.3% per transaction. The Uniswap protocol automatically adds the fees mentioned above to the liquidity reserve, and the providers can redeem them at any time. The fees are distributed according to each liquidity provider's share of the reserve.

The UNI token

UNI is the native token of the Uniswap protocol and gives its holders governance rights over the network. This means that only

UNI holders are allowed to vote regarding changes to the protocol. One billion UNI tokens were minted at the creation of Uniswap, and 60% of these were distributed to existing members of the Uniswap community. In contrast, the remaining 40% are made available to team members, investors, and consultants. This 40% will be released in small bunches over four years to avoid large fluctuations in UNI's price.

Impermanent loss

Impermanent loss occurs when you provide liquidity to a pool and the cryptocurrency price changes after the deposit; the more significant this change, the greater the impermanent loss. In this case, loss means a reduction in the dollar value at the time of withdrawal compared to the time of deposit.

Pools containing cryptocurrencies that remain in a relatively narrow price range are less exposed to impermanent losses: stablecoins, for example, stay in a somewhat limited price range and therefore offer a lower risk of

impermanent loss for liquidity providers.

But why do liquidity providers still provide liquidity if they are exposed to potential losses? Because any impermanent loss can be neutralized by the fees earned. Even pools on Uniswap that are pretty exposed to impermanent losses can be profitable thanks to commissions earned. For example, suppose there is a large trading volume in a given liquidity pool. In that case, it can be profitable to provide liquidity even if one is highly exposed to impermanent losses.

Let us examine a concrete case of how a impermanent loss can occur for a liquidity provider.

Marie deposits 1 ETH and 100 USDT in a particular liquidity reserve. In this specific market maker, the deposited token pair must be of equivalent value (as on Uniswap): this means that the price of 1 ETH is comparable to 100 USDT at the time of deposit. This also implies that the dollar value deposited by Marie is 200. Let's assume further that there are 10 ETH and 1,000 USDT in the pool deposited by other liquidity providers. Thus,

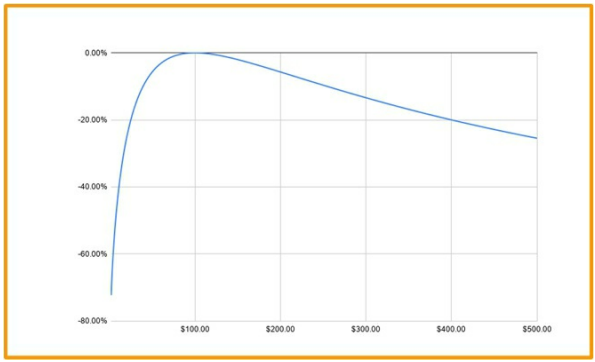
Marie has a 10% stake in the pool, and the total liquidity in the said pool is 10,000.

Let's assume that the price of ETH rises to 400 USDT. As this happens, traders will add USDT to the pool and remove ETH until the ratio reflects the market price. It must be remembered that what determines the cost of the assets in the pool is their ratio within the same pool. While liquidity should remain constant, the ratio of cryptocurrencies in it changes. If ETH is now worth 400 USDT, the percentage of how much ETH to how much USDT is in the pool has changed: there are now 5 ETH and 2,000 USDT in the pool, thanks to transactions made by traders.

To continue this example, let's assume that Marie decides to withdraw her funds. As we know from before, she is entitled to a 10% share of the cash pool. As a result, she can withdraw 0.5 ETH and 200 USDT for a total value of 400 USD. With only 200 deposited, this is a remarkable increase. But what would have happened if she had kept the ETH and 100 USDT in her wallet? The dollar value following the ETH price change would now

be USD 500. In short, by putting her funds in the cash reserve, Marie has lost $100 in value. This loss is precisely temporary.

The graph below shows the percentage loss as the price of ETH changes with $100 as a starting point. As can be seen, a fall in the price of ETH leads to a rapid impermanent loss, while an increase in the price allows for a more progressive impermanent loss.



To recap

- Decentralized finance seeks to expand the use of blockchain from a case of simple value transfer to more complex financial services.
- Uniswap is a decentralized exchange and a market maker.

- Automated market makers are smart contracts that hold cash reserves with which traders can exchange cryptocurrencies.
- Anyone can provide liquidity to Uniswap.
- Providing liquidity may result in an impermanent loss.

Chapter 15 - Yearn Finance

An essential premise is to be made: even though it may be evident at this point, this book does not primarily concern itself with investing in cryptocurrencies but rather understanding their technical workings. Another side of the coin is the apparent link between the two issues. To invest, you need to know what you are investing in. However, having talked about liquidity pools, impermanent loss, and decentralized finance, one cannot continue on this path without considering Yearn Finance and its YFI token. This token has already been mentioned in chapter 9, speaking of understanding the capitalization of a cryptocurrency. Here we can go into more detail.

In the example shown in the previous section, we saw how Marie lost value by providing liquidity to the ETH/USDT pool. However,

had Marie been able to foresee the impermanent loss and the risk associated with this specific liquidity pool, she could have acted differently and perhaps managed to reduce or eliminate the loss. Yearn Finance has precisely this purpose: to enable liquidity providers to choose the pools with the best return and the lowest risk.

Launched by Andre Cronje in early 2020, Yearn finance is also an ERC-20 token based on Ethereum. Unfortunately, the smart contract was hacked shortly after its launch, and $2.5 million were stolen. Following this event, the developers worked to increase security, and since then, there have been no successful hacking attempts.

The primary function of Yearn Finance is known as the *Vault*, and it allows users to deposit cryptocurrencies and earn returns automatically. The deposited funds are managed autonomously by an algorithm that seeks to maximize profits and minimize risk by choosing liquidity pools with precise characteristics. When the service was launched, it focused primarily on stablecoin

liquidity pools; however, over time, it has been expanded to include pools featuring Ethereum, Chainlink, and other cryptocurrencies.

An exciting feature of the Vault is its caDCAity to mitigate the high cost of transactions on Ethereum; by pooling capital with other users, only the Vault's controller account has to pay transaction fees to provide liquidity.

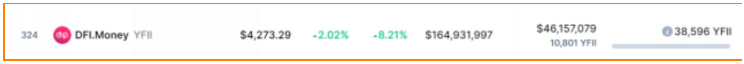
Yearn Finance's range of offerings also includes minor services, which we mention for information purposes only. Most of the annuities are obtained from the Vault. The other products are:

- Earn, which is essentially a version of the Vault that only includes stablecoins;
- Zap, which allows stablecoins to be exchanged for other tokens;
- yInsure, which offers decentralized insurance coverage;
- StableCredit, which facilitates the decentralized lending of stablecoins.

The YFI token

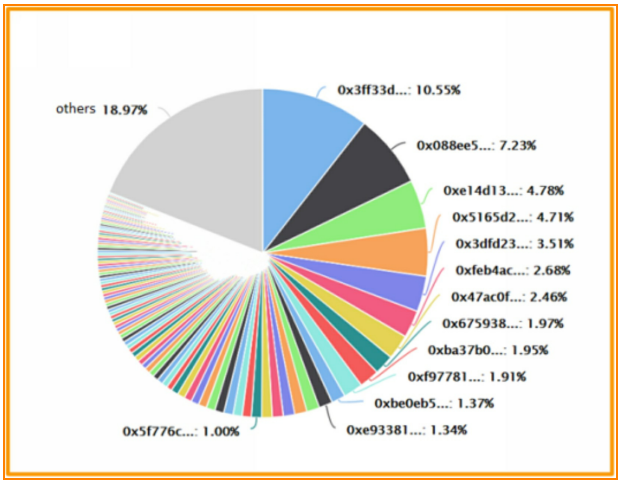
Until July 2020, Yearn finance was instead a niche and only known by very few. Moreover, after the exploit in early 2020 and the subsequent market crash in March, many users were reluctant to confide in the new protocol. That changed when Cronje published a post on Medium announcing YFI, an ERC-20 token launched so that users themselves could rule the Yearn finance protocol. Despite Medium's post explicitly stating that YFI has no intrinsic value and only plays a protocol management role, the market continued to increase its price. In little more than a month, YFI went from $3 to $3,000 in investor euphoria. To date, this is one of the most impressive rises ever recorded in the cryptocurrency world. Shortly after the token's launch, the community used the power of governance to limit the maximum number of YFIs to just 30,000 coins. Users dissatisfied with this decision performed a hard fork, creating Yearn Finance 2 (YFII). However, as you can see, YFII has not been very successful and is used

by very few people.



Although many focus on the price of YFI, it is essential to note that its introduction marked a change in the way specific protocols can incentivize the adoption of a token. YFI's is seen by many as the fairest launch since Bitcoin, as anyone could participate in generating the coin by paying the same price. Instead of doing the classic ICO, where users pay a specific price for the new coin, Yearn Finance users had to use the protocol to receive YFIs. This mechanism allowed for the rapid formation of a community. Each user had the same ability to influence the Yearn Finance protocol through the token.

Indeed, looking at the image, one can see that most tokens are not in the hands of a few significant addresses.



Yearn Finance is the most direct way for cryptocurrency investors to generate an income on their capital decentralized. As an investment, risks are inevitably involved. Still, the choice is pretty straightforward between providing liquidity to a pool on your own or relying on a service with a proven track record of delivering positive results. Using Yearn Finance is quite intuitive and straightforward. In this case, as seen in some others previously, we will not report a tutorial since the key's position could change at any given time. We, therefore, refer the reader to the protocol's official website (yearn.finance).

To recap

- Yearn Finance allows users to delegate the choice of the best cash reserves.
- The Yearn Finance algorithm can minimize impermanent loss and maximize profits.
- The launch of Yearn Finance was very democratic, and therefore the token is distributed to many different addresses.
- Yearn Finance, like all investments, has a percentage of risk.

Chapter 16 - Basic Attention Token (BAT) and Utility Tokens

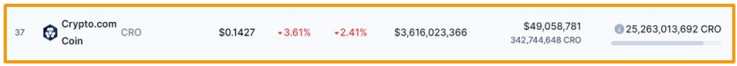
Decentralized finance is not the only area where Ethereum applications can be helpful. This is, in fact, a relatively new area, although it is the one with the highest degree of possible expansion. The second area where Ethereum's smart contracts come in very handy is in utility tokens.

Utility tokens

A utility token is a digital asset used to finance the network to which it belongs, providing its holders with a guarantee that they will be able to use some of the services offered by the project in question or granting them advantages over those who do not own that token. All utility tokens rely on a third-party blockchain, such as Ethereum's, and

therefore cannot be produced through mining.

Utility tokens are often used in ICOs: developers raise the necessary funds to carry out the project, giving a token in return that will allow its owner to have particular advantages when the network becomes active. As a result, the real value of a utility token lies not in the possibility of speculating on the price but in what it allows you to do. Many exchanges have launched their utility tokens in recent years. These tokens usually allow for a reduction in transaction fees and the possibility of receiving benefits such as a debit card associated with your account. In particular, this is the case with the token on the Crypto.com exchange (crypto.com).



For the record, it is worth noting that CRO does not operate on the Ethereum blockchain; Crypto.com has created its blockchain for its users to operate on.

Binance also has its utility token, called BNB, an ERC-20 token for several years and is thus based on the Ethereum blockchain. However, in 2020 Binance announced the creation of a proprietary blockchain, the Binance Smart Chain, to which BNB migrated. Lastly, BNB can reduce commissions on trades and access some of Binance's services with more favorable prices.

Both CRO and BNB are centralized utility tokens. It is clear that the main reason for their existence is to allow the two exchanges to raise capital. Basic Attention Token, on the other hand, serves a different purpose.

Basic Attention Token

Designed by Brendan Eich, creator of Javascript and co-founder of Mozilla.org, Basic Attention Token (BAT) aims to decentralize one of the web's most significant elements: advertising. BAT, therefore, seeks

to reward users and content creators based on the attention they capture. Hence, the token is distributed to users based on their online activity and to content creators based on how much interest they receive.

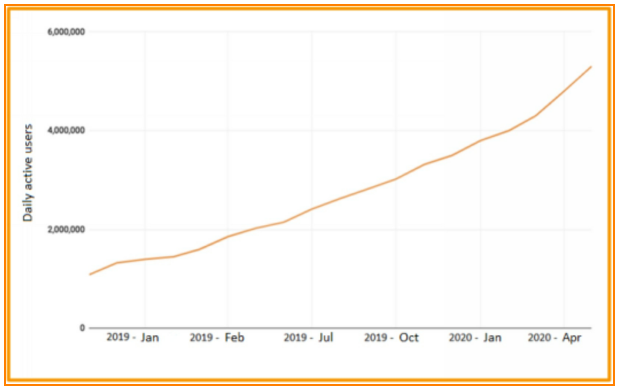
The BAT token is only available on the Brave browser (brave.com), which uses Chromium as its base and is very similar to Google Chrome in terms of interface and functionality. Brave blocks third-party ads that have not used BAT to buy advertising sDCAe to allow this decentralization of advertising.

After downloading the Brave browser, users can activate the Brave Rewards function, which allows them to earn BAT by surfing Brave and viewing ads. Users can also send part of their BAT to their preferred content creators.

BAT transfers within Brave are made through the Uphold platform. An interesting aspect is that Uphold itself covers the gas cost of the transfers.

BAT is designed to solve the problems that online advertising has failed to solve in the ongoing transition from desktop to mobile. Although websites are now prepared to display correctly on mobile devices, advertisements cannot always be said, which can significantly slow down the browsing experience. It can be estimated that in 2020 advertisements cost users up to 23 dollars per month in data and electricity, as they drained 21% of mobile phone batteries. On the other hand, traditional publishers are also losing advertising revenue due to the ongoing technological change. Brave and BAT want to introduce a new system that is more rewarding for all parties involved.

Brave's adoption rate is on an ongoing positive trend, and recently the browser exceeded 25 million monthly active users. The graph below shows the usage curve from 2019 to 2020 in terms of daily active users.



For technology enthusiasts, Brave is definitely worth a try.

To recap

- A utility token is a digital asset used to fund the network it belongs to.
- Many exchanges have launched their utility tokens in recent years.
- Basic Attention Token wants to decentralize online advertising.
- The BAT token can be used to reward your favorite content creators using the Brave software.
- Brave has just surpassed 25 million

monthly active users.

Chapter 17 - NFTs: Another Token Standard

So far, we have only looked at decentralized applications that follow the ERC-20 standard. However, these are not the only smart contracts built on the Ethereum blockchain: another necessary standard is ERC-721, which identifies non-fungible tokens (NFTs).

An NFT is a unique unit of data stored on the blockchain which can be sold and traded. The NFT can be associated with, and therefore represent, a particular digital or physical asset, such as an image or real estate. NFTs function similarly to the ERC-20 tokens we have seen so far, but, unlike them, NFTs are not mutually interchangeable: they are therefore non-fungible.

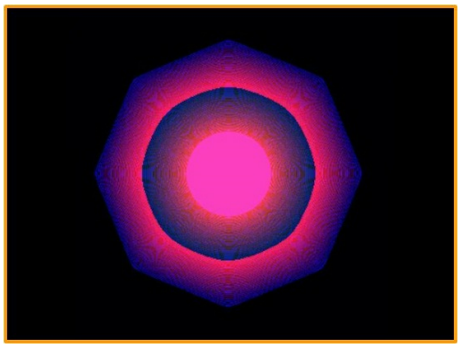
For example, although all BATs are the same, and therefore it does not matter which of the 417 million units in circulation a user owns, each NFT represents a different underlying asset and therefore has an additional value.

NFTs are created using a hash function on a file that certifies ownership of a specific object on a technical level. This process guarantees the authentication of each file. In addition, it provides a digital signature used to track the ownership of the token. This process is also called 'minting.' It allows the owner of an object outside the blockchain to be carried onto it.

Moreover, as the blockchain is a public register, anyone can see which address a given NFT belongs to. It may happen that, due to the large file size, NFTs are not stored directly on the blockchain. In those cases, the token is associated with a web address that leads to the artwork in question.

The history of NFTs

The first NFT, called Quantum, was created on 3 May 2014 by Kevin McCoy and Anil Dash, live at the Seven on Seven conferences at the New Museum in New York City. For the young cryptocurrency industry, this was a defining moment.



In October 2015, the first full-fledged NFT project called Etheria was launched at DEVCON 1, Ethereum's first developer conference, just three months after the launch of the blockchain itself. It was a game in which users could buy, modify and sell pieces of a virtual world. Each of Etheria's 457 NFTs initially sold for one ETH, which at the time was worth just under a dollar. However, most remained unsold for more than five years until 13 March 2021, when renewed interest in NFTs sparked a buying frenzy. In just 24 hours, all NFTs were sold for a total of $1.2m.

In 2017, American studio Larva Labs released the CryptoPunks collection. This project allows the exchange of unique stylized characters on the Ethereum

blockchain. As a result, 10,000 CryptoPunks have been created, and many consider this the first actual case of NFT in history. Initially, CryptoPunks were sold for derisory amounts of money. Today, however, some Punks are worth over a million dollars. As seen in the image below, it is not necessarily the aesthetic quality of the artwork that determines the price: historicity, rarity, and market euphoria are the factors that most influence the value of an NFT.

In 2021 NFTs have seen a considerable increase in interest, and major brands such as Nike and Vaynermedia have entered the sector. To be fair, this is the application of blockchain that has garnered the most

institutional attention.

Common use cases

Digital art was one of the first use cases of NFTs. The digital artwork entitled "Everyday - The First 5000 Days" by artist Mike Winkelmann, also known as Beeple, was sold for $60 million in 2021. This was the third-highest auction price ever achieved for a living artist, after Jeff Koons and David Hockney. Another Beeple piece entitled "Crossroad," consisting of a 10-second video showing animated pedestrians walking in front of a Donald Trump figure, sold for $6m on Nifty Gateway (niftygateway.com), an NFT exchange. The image below shows the thumbnail of the video.

Also interesting is the case of the work "Mars House," a 3D model of a house on the red planet created by artist Krista Kim, which was sold as an NFT for over $400,000.

NFTs can also represent collector's items, a bit like stickers, but in a wholly digital format. For example, in February 2021, LeBron James' slam dunk NFT from the NBA Top Shot collection was sold for over $200,000.

Another area in which NFTs can be successfully deployed is gaming. In this case, non-fungible tokens represent resources within the game, such as digital plots of land controlled by the user instead of the game developer. The interoperability of the

blockchain, in this case, makes it possible to transport the same object from one game to another, thus enabling the emergence of new gaming ecosystems in continuity with each other. Sandbox is one of the first projects that try to do just that: it's attempting to create a network of games in which the user can dispose of their resources in each of them.

NFTs have also been used successfully in the music sector: they allowed musicians to tokenize their work, expanding the list of options to monetize and profit from their music. To understand the scale of this phenomenon, NFTs generated around $2 million in the music industry in February 2021. On 28 February 2021, musician 3LAU sold a collection of 33 NFTs for a total of $11 million to commemorate the third anniversary of the release of his album 'Ultraviolet.'

It should be noted that ownership of an NFT does not inherently guarantee copyright in the digital resource represented by the token. While an artist may sell an NFT representing their work, the buyer will not necessarily receive rights beyond ownership of the

specific piece of art. This allows the artist to create multiple NFTs of the same work. Furthermore, it is fair to point out that not all NFTs are built on Ethereum: some projects also rely on other blockchains, such as the Binance Smart Chain, Flow, and Tezos.

Buying and selling NFTs

Non-fungible tokens cannot be purchased on most traditional exchanges. For example, Coinbase does not yet offer this possibility. There are, however, platforms that specialize in this market: these include Opensea (opensea.io), Rarible (rarible.com), and Super Rare (superrare.com).

Opensea is the marketplace that offers the largest selection of NFTs, offering anyone the possibility to create and sell their works. However, while this approach allows small artists to bring their creations to the blockchain, it does not allow them to gain broad exposure due to the vast supply.

Rarible and Super Rare, on the other hand, are niche exchanges reserved for artists and projects of a certain caliber. These are the two platforms where the most expensive purchases and sales occur, and any artist who wants to "breakthrough" in this sector looks to these two marketplaces as a point of arrival. But, of course, the selection of works is made by the companies' management, making the most traditionalists of the blockchain philosophy turn up their noses.

To recap

- NFTs on Ethereum follow the ERC-721 standard.
- An NFT is a single unit of data stored on the blockchain.
- The first NFT was called Etheria and was launched in 2015.
- NFTs can represent works of art, collectibles, physical assets, and holdings.
- NFTs can be bought and traded on Opensea, Rarible, and Super Rare.

PART 4 - BEYOND ETHEREUM

Chapter 18 - Cardano and the Academic Approach to the Blockchain

Ethereum is not the only alternative blockchain to that created by Bitcoin, even though it is the one upon which most decentralized applications are built. Among the competitors of Vitalik Buterin's project, the one with the largest capitalization is Cardano, with its ADA token.

Cardano has generated a lot of interest since its creation in early 2015. The academic rigor applied to its development makes Cardano somewhat unique in the cryptocurrency sDCAe, which is often driven more by enthusiasm than a clear entrepreneurial vision. The Cardano project was primarily developed by Input Output Hong Kong

(IOHK), founded by Charles Hoskinson. He, if we remember, was also involved in the development of the Ethereum project. A scientific and logical approach is used in the continuous development of the platform; according to its creators, the fundamental design principles behind Cardano are security, scalability, and interoperability.

Cardano's development of consists of five main phases:

- Byron;
- Shelley;
- Goguen;
- Basho;
- Voltaire.

Byron marked the launch of the network along with basic functionalities, such as the possibility to transfer ADA from one address to another. The Shelley phase took place in 2020 and brought significant improvements on the decentralization side, putting the management of network nodes in the hands of ADA holders. The Goguen phase will

enable the introduction of smart contracts on Cardano's blockchain, while the Basho phase will optimize the scalability and interoperability of the blockchain. Finally, the Voltaire phase will introduce a treasury system, which will make Cardano one of the most secure blockchains in the world.

Cardano's systematic approach makes it a 'third generation' blockchain, whose aim is to solve the scalability problems still present within the first (e.g., Bitcoin) and second generations (e.g., Ethereum). According to proponents of this classification, blockchains of previous generations have deep-rooted problems within the code that limit the number of transactions they can handle. This makes them an inefficient choice for mass adoption. To compare, Cardano's white paper is more analog to VISA's computing power: "the network reportedly handles an average of 1,736 payment transactions per second (TPS) with the caDCAity to handle up to 24,000 TPS."

Cardano aims to improve scalability in several ways. One of the most significant

pillars of this goal is their proprietary Proof of Stake (PoS) consensus mechanism, called Ouroboros. Ouroboros reduces energy costs compared to Proof of Work (PoW) systems while providing significant security. In addition, Cardano's Layer 2 solution for further scalability, Hydra, is named after the mythological creature. The idea of Hydra is that the number of transactions can increase as new nodes are added to the network.

As previously mentioned, Cardano's strength lies in its underlying academic and scientific philosophy. The development team has published more than 90 white papers to define and catalog the underlying technology. The project has a well-defined roadmap, although the timetable has not always been respected. As can be seen in the image, the initial idea was to complete the development of the five phases by 2020; however, as of September 2021, the Goguen phase has yet to be completed.

The ADA token

ADA is Cardano's token and is named after 19th-century mathematician Ada Lovelace. 57.6% of ADA was distributed in an ICO in late 2016, through which Cardano raised over $60 million. The token can be used both as a digital currency and to make transactions on Cardano's network. ADA holders also have a stake in Cardano's blockchain: this stake can generate rewards through Proof of Stake.

Not being an ERC-20 token, ADA cannot be held in a wallet with an Ethereum address. Developed by Input Output Hong Kong itself, Daedalus (daedaluswallet.io) is the most widely used software wallet designed to hold ADA. It is a full node wallet. The entire Cardano blockchain must be downloaded, and every transaction must be verified for

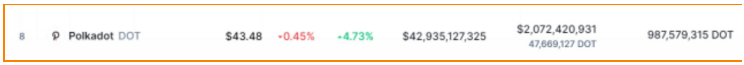
maximum user security. There are also light node wallets, such as Yoroi (yoroi-wallet.com) and AdaLite (adalite.io), which do not require the entire Cardano blockchain to be downloaded. In addition, the ADA token can also be stored on hardware wallets, such as Ledger and Trezor.

To recap

- Cardano is a competitor to Ethereum.
- Cardano's systematic approach makes it a third-generation blockchain.
- Cardano's development is divided into five phases: Byron, Shelley, Goguen, Basho, and Voltaire.
- Cardano uses a Proof of Stake consensus mechanism.
- The ADA token can be used as a digital currency and carry out transactions on Cardano's network.

Chapter 19 - Polkadot and the Concept of Parachain

Like Cardano, Polkadot wants to be the next step in adopting blockchain technology, focusing its efforts on security, scalability, and innovation. To do this, it is necessary to create the infrastructure needed to support new ideas and concepts and ensure proper interoperability between blockchains. The protocol was initially conceived by Gavin Wood, co-founder of Ethereum; as you may have noticed, it is not uncommon for the same developers to have worked on multiple different cryptocurrencies.



Polkadot is the first protocol that actively tries to make multiple blockchains communicate with one another. This advantage lies in the possibility of using the same decentralized application on numerous

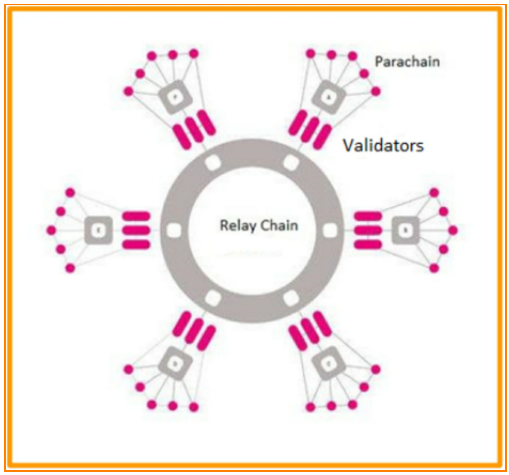
networks, with continuity and consistency.

For example, on the Polkadot platform, each of the cryptocurrencies we have examined so far could have its blockchain and collaborate directly with all the others. In technical jargon, this is referred to as 'cross-chain interoperability. On a technical level, this is not easy to achieve. Let's dive into the structure behind this idea.

A single blockchain in the Polkadot ecosystem is called a parachain, or "parallel blockchain," while the main chain is known as a "relay chain"; the idea is that each parachain can easily exchange information with the relay chain at any time. Any developer, company, or individual can start their custom parachain via the proprietary Substrate framework, enabling the creation of cryptocurrencies and decentralized systems. Once the custom blockchain is connected to Polkadot's network, it becomes interoperable with all other parachains on the web.

The creation of cross-chain applications, products, and services should become much easier with this structure. The protection and

validation of data across parachains are done through network validators, where a small set of people can validate multiple parachains simultaneously. These validators will also ensure that transactions can be distributed across numerous parachains to improve scalability and transactions per second. The following image graphically illustrates this concept.



There are be many reasons why developers should use the Polkadot ecosystem. In fact, due to the limited nature of current blockchains, it is abundantly clear that there are some fundamental issues that a decentralized application programmer has to

deal with: scalability, customization, and interoperability.

On the scalability front, by acting as a multi-blockchain network Polkadot allows transactions to be processed in parallel across multiple parachains. This removes one of the biggest hurdles associated with blockchain technology today. Parallel processing is a significant improvement and can pave the way for greater global adoption of this technology.

Looking instead to the customization of decentralized applications, the idea that there should be a single standard on which to base smart contracts is completely dropped on Polkadot. Each project has its requirements, and Polkadot allows each parachain to have a design optimized for its specific functionality. With the help of the Substrate framework, developers can efficiently adapt their parachains to the project's needs and not have to limit their application to comply with the rules of more stringent standards.

Lastly, on the interoperability front, having projects and applications continuously share

data is an essential factor. While it remains to be seen what kind of products and services will be created on Polkadot, several use cases have already emerged. For example, decentralized finance finds new life, as interoperability would allow for different parachains, each dealing with a specific aspect of finance, to communicate with each other cohesively. Any application associated with a particular parachain will be able to govern its network as it sees fit; moreover, all applications are crucial to the overall governance of the Polkadot protocol.

The DOT token

Like most other blockchain infrastructure projects, Polkadot has its native token, called DOT, which serves the same function as ETH for the Ethereum project. Firstly, it allows owners to participate in decisions related to the development of the ecosystem, including the determination of transaction fees and the implementation or removal of any given parachain. In addition, DOT is designed to

facilitate network consensus through staking. As with Ethereum 2.0, all DOT holders are incentivized not to sell their tokens, as these can be used to validate blocks in exchange for a reward. Finally, DOT is used as a tool for activating parachains; when a decentralized application wishes to start its network on Polkadot, it will have to block a certain amount of DOT to complete the operation.

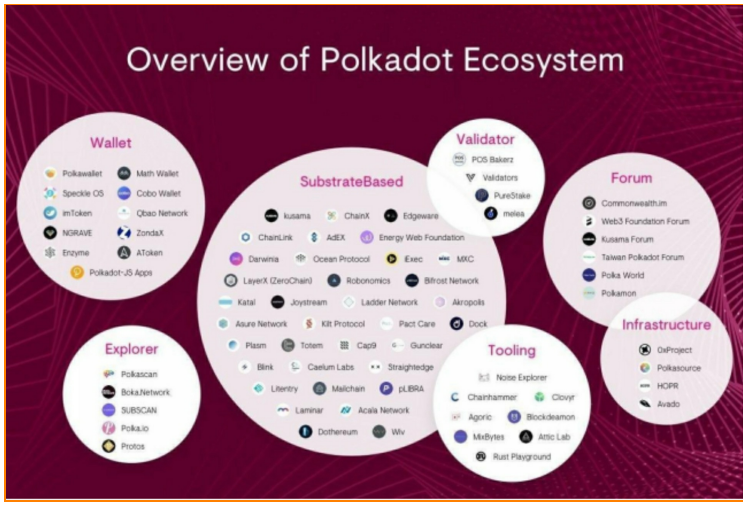
The DOT token must be stored in a specific wallet. Apart from the classics Ledger and Trezor, which also support Polkadot, various software alternative wallets exist. The most widely used of these are PolkaWallet (polkawallet.io), MathWallet (mathwallet.org), and TrustWallet (trustwallet.com).

The Kusama network

Polkadot was the first protocol to integrate a secondary chain, in which developers can test and process decentralized applications before launching a parachain. This test network is called Kusama, and KSM is it's token.

Kusama's main objective is to create a virtuous environment in which to test innovative or rapidly-built projects and carry out pre-checks before deploying applications on Polkadot. However, it is essential to note that this is not a test network; if the application works correctly, there is no need to move it to Polkadot. Instead, developers can decide to work exclusively with Kusama through a parachain governed by KSM token holders.

As we did for Ethereum, you can see the significant applications developed on the Polkadot protocol in the image below. Although large, it is still a smaller ecosystem than Ethereum. This is because it is a relatively young project which has only recently caught the attention of developers of decentralized applications.



To recap

- Polkadot is the first protocol that makes multiple blockchains communicate with each other.
- The leading blockchain is called a relay chain; the secondary ones are known as parachains.
- Validators add blocks to the relay chain, simultaneously validating all parachains.
- The DOT token is used to activate parachains, perform transactions on the

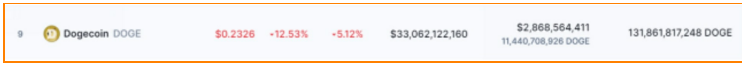
network, and staking.

- Kusama is Polkadot's secondary network and is used to experiment with new parachains.
- If the application tested on Kusama is working correctly, there is no need to move it to Polkadot.
- KSM has the same functions as DOT.

Chapter 20 - Dogecoin and Meme Coins

The cryptocurrency industry has proven to combine the seriousness required for creating a decentralized financial system with the humor and informality typical of technology and programming enthusiasts.

For example, the name 'Uniswap' includes an apparent reference to unicorns. This is not an uncommon occurrence. After all, browsing through the pages of CoinMarketCap, one comes across tokens called "Shiba Inu," "SushiSwap," "Safemoon," "PancakeSwap," and other similar nicknames. Despite the widespread use of this lively terminology, the first blockchain project to introduce a humorous aspect was Dogecoin with its DOGE token.



As the name suggests, this cryptocurrency is primarily based on the Doge meme that took

the internet by storm in 2013. The original image depicts a dog of the Shiba Inu breed, whose rather amusing internal monologue is written in comic sans font.

Billy Markus, a programmer from Oregon, and Jackson Palmer reasoned that a 'less serious' currency would better attract mass attention than Bitcoin. Billy and Jackson were right: upon launch in 2013, the cryptocurrency spread like wildfire all over social media. In just a few months, Dogecoin reached a multi-million dollar market capitalization and has since continued to expand, following the market in both good and bad times.

Dogecoin belongs to the category of

'memecoins, cryptocurrencies that have no actual use other than to put a smile on the face of those who come across them for the first time. DOGE has a very high inflation rate. Thirty thousand new DOGEs are issued with each block. This is why, to date, Dogecoin's outstanding balance is over 1000 billion.

Although DOGE has no defined purpose, its community has gained a good reputation for significant charitable work overtime. Initially, Dogecoin was used as a tipping system on Reddit. Users would exchange small amounts of Dogecoin for rewarding content creators. Essentially, this is the same thing Basic Attention Token aims to do now.

In 2014, the community raised over $30,000 in Dogecoins for the Jamaican bobsleigh team, enabling them to compete in the Sochi Winter Olympics. Unfortunately, the team qualified but could not afford to travel to Russia for the event. Nevertheless, it was a gesture picked up by well-known newspapers and shed some positive light on the whole industry, which did not bask in a good

reputation. The same year, the community also launched the Doge4Water initiative, which raised $30,000 to create water wells in Kenya.

However, the actual market buzz only began to build in the mid-2020s, when a viral video on TikTok created a chain reaction, causing the price of DOGE to rise significantly. In the video, the influencer asked his followers to join him in buying Dogecoin, stating that they would all become rich by purchasing DOGE and selling it once the price reached a dollar. This doubled the price in just two weeks, even though DOGE never reached the dollar mark.

Interestingly, this practice could be considered price manipulation if it were a regulated market. In fact, this type of behavior is illegal in traditional markets because of the dangers to investors. Promoters buy large quantities of an asset before generating FOMO (*fear of missing out*), inducing others to invest. As a result, the price increases significantly. Subsequently, promoters sell their shares at a

considerable profit to the detriment of those who followed them in purchasing the shares mentioned above.

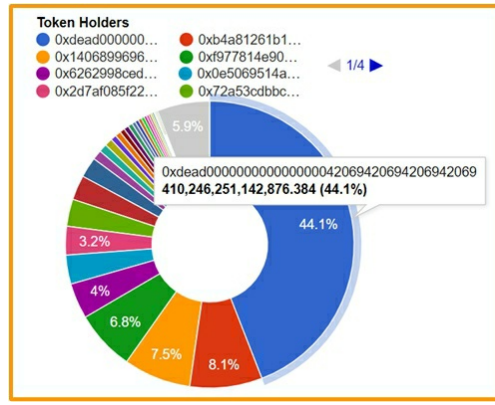
Following the success of Dogecoin, many other 'memecoins' were born, such as Shiba Inu, Woofy, Banano, Polkadog, Dogelon Mars, and Cake Monster. However, two things distinguish DOGE from all the others:

- The distribution of tokens is not exclusively in the hands of a few addresses;
- The organic growth of the community, not based solely on momentary euphoria.

As you can see from the chart below, most of DOGE is controlled by a huge amount of addresses.

N° of DOGE	N° of addresses	% of addresses
(0 - 0.001)	297161	6.86% (100%)
[0.001 - 0.01)	7753	0.18% (93.14%)
[0.01 - 0.1)	36374	0.84% (92.96%)
[0.1 - 1)	57418	1.33% (92.12%)
[1 - 10)	1061244	24.5% (90.8%)
[10 - 100)	854726	19.73% (66.3%)
[100 - 1,000)	1120732	25.87% (46.57%)
[1,000 - 10,000)	636279	14.69% (20.7%)
[10,000 - 100,000)	222314	5.13% (6.01%)
[100,000 - 1,000,000)	33410	0.77% (0.88%)
[1,000,000 - 10,000,000)	3865	0.09% (0.11%)
[10,000,000 - 100,000,000)	640	0.01% (0.02%)
[100,000,000 - 1,000,000,000)	78	0% (0%)
[1,000,000,000 - 10,000,000,000)	11	0% (0%)
[10,000,000,000 - 100,000,000,000)	1	0% (0%)

On the contrary, if we look at the picture in Chapter 10, we can see that most of the SHIB tokens of the Shiba Inumemecoin are in the hands of very few entities. Analyzing the distribution of all the other memecoins mentioned above, we can see that the percentages are more or less similar.



To recap

- "Memecoins" are cryptocurrencies that have an exclusively humorous purpose.
- Dogecoin was the first memecoin and was created in 2013 by Billy Markus and Jackson Palmer.
- Over the years, the DOGE token has been used for charitable endeavors.

- Dogecoin has a very high circulation as 30,000 DOGE are issued per block.
- In times of market euphoria, many memecoins tend to appear.
- As memecoins have no purpose, they are very risky for investors.

PART 5 - INVESTING IN CRYPTOCURRENC

Chapter 21 - False Myths about Cryptocurrency Investing

Before delving into the more technical side of this guide, it's necessary to analyze and debunk some false myths about investing in cryptocurrencies. All too often, new 'investors,' fearful of missing out on an opportunity, start buying and selling coins without the awareness needed to make decisions best tailored to their situation. Investments (in any market) must be thoroughly thought out and implemented based on an objective, which depends on the investor.

For example, a 38-year-old man in Milan with a good job and a house will have different needs and possibilities than a university student with a thousand dollars to spare. That means that to propose a universal approach to investing in cryptocurrencies is difficult and counterproductive.

That's why in this guide, the investor we will reference has some well-defined characteristics:

- Has a steady income that allows them to have a surplus of money at the end of the month;
- Has a liquid emergency fund equal to at least six months of their lifestyle;
- Wants to invest in the long term.

If we have done our marketing job correctly, you should recognize yourself in this description. So let's now look at the false myths our typical investor is likely to have heard about this sector.

The risk of investing in bitcoin

This is neither a myth nor a false one. Like any investment, investing in Bitcoin and cryptocurrencies involves risk. We can define financial risk as to the possibility that there will be a depreciation of the invested capital in a limited period. For example, if you had bought Bitcoin in December 2017, you would

have had an 80% depreciation of your wealth after one year.

However, extending the time period to just over three years would have resulted in an appreciation of over 100%.

This means that the length of time one remains invested plays a crucial role in financial risk management. Similar examples could be given for any market. In March 2020, the S&P 500 (the index tracking the 500 most capitalized US companies) lost roughly 36% over a couple of months.

However, over a longer period of time, there would have been a capital appreciation in this case as well.

If you are familiar enough with the subject, you will know that the S&P 500 has consistently grown in value over the long term. On average, it has returned 12% annually over the last 40 years. It is easy to see that the financial risk for this index is exclusively time-dependent. If you wait long enough, you have an excellent chance of positive investment. One wonders if this is also the case for Bitcoin. Can one

significantly lower the financial risk of Bitcoin simply by staying invested for long periods? The data, in this case, gives us an obvious answer.

From 2010 to the present day, it can be seen that the price of Bitcoin has continued to rise, rewarding those who have stayed invested longer. In this sense, Bitcoin has trended similarly to the S&P 500 in that the more time that passes from the time of purchase, the more the financial risk decreases.

For example, it is clear that for those who bought Bitcoin in 2010, today, the risk of seeing their capital depreciate below the value initially invested is virtually zero.

We can, therefore, "correct" this false myth:

Investing in Bitcoin is risky → Investing always involves financial risk. However, like

the S&P 500, Bitcoin has proven to be an asset whose financial risk decreases as time passes from the time of investment.

You should invest a maximum of 10% of your net worth in cryptocurrencies

This myth is debatable because it does not take into account the investor's profile. As we said earlier, any attempt to give universal rules is a failure for investments. For example, suppose it was always true that cryptocurrencies cannot count for more than 10% of an investor's portfolio. In that case, there should also be a universal rule about allocating the remaining 90%. However, you only have to read any book dealing with investments to realize no unanimously agreed percentages.

For example, Warren Buffett's most prominent position is Apple, which counts for 40% of his company's portfolio, Berkshire Hathaway; on the contrary, Ray Dalio's

largest allocation is in the S&P 500 and counts for only 5.42% of the total capital. So we are talking about two of the most prominent investors globally, and there is still no common thread.

This is why you should not invest more than 10% in cryptocurrencies is simply untrue: 10% may be too much for some and too little for others. Against the backdrop of data we have collected and the performance of Bitcoin compared to that of the US stock market, we can say that the investor profiled at the beginning of this chapter can go as high as 20%, allocating the remaining 80% of their capital in ETFs on the US stock market.

From December 2017 to August 2021, Bitcoin grew by 273%, while the S&P 500 rose 66%. This means that a portfolio with the 80/20 allocation would have had a total growth of around 107% in just over three years, averaging 35% per year. If you had limited yourself to 10% in Bitcoin, the total growth would have been "only" 80%, with an annualized return of just over 20%. That extra 10% allocation would have cost the investor

15% per year.

So let's dispel this myth:.

You should invest a maximum of 10% of your capital in cryptocurrencies. → There is no universal rule. For the investor profiled at the beginning of this chapter, we recommend going as high as 20%.

Trading cryptocurrencies is more profitable than investing in them.

This myth is the one responsible for the most significant losses of invested money ever. No statistic shows that cryptocurrency trading is more profitable than passive investing. Instead, according to numerous sources, 90% of traders perform less well than the asset they are trading. This begs the question as to why anyone would be willing to get slaughtered by the market. The answer is simple and goes back to the first false myth we mentioned: traders try to mitigate

financial risk by guessing when to exit and when to enter. However, as we have seen, in an asset like Bitcoin, it is time itself that reduces this risk. Investing is, therefore, a much more profitable way to earn a return on investments in this market.

Trading cryptocurrency is more profitable than investing → 90% of traders lose money compared to passive investors.

Now that these false myths have been debunked, we can technically talk about investing in cryptocurrencies.

To recap

- Investing in cryptocurrency is no riskier than investing in other assets.
- The 10% rule is not valid: it depends on the investor's profile.
- Investing is statistically more profitable than trading.

Chapter 22 - The Bitcoin "Dominance"

Just as the stock market tends to move in unison thanks to indices, cryptocurrencies also have a correlated trend. Bitcoin dominates in this sector: when it rises in price, it takes the whole market with it, and when it falls, there are hardly any cryptocurrencies with a positive performance. It should be noted that the correlation is amplifying: other cryptocurrencies (also known as 'altcoins') tend to rise and fall in more significant percentages than Bitcoin.

The correlation between Bitcoin and other currencies is given by a proportion called 'dominance.' This is obtained by dividing the total market capitalization of cryptocurrencies by the capitalization of Bitcoin. This gives a percentage, which expresses how much Bitcoin influences the market. Indeed, dominance expresses the percentage of new funds that are allocated to Bitcoin compared

to other cryptocurrencies. For example, with a dominance of 99%, in 2014, 99 dollars out of 100 were invested in Bitcoin.

As you can see from the monthly chart, Bitcoin's dominance trend is bearish. This means that the more this sector matures, the more the price trend of the individual cryptocurrencies diverges from that of Bitcoin.

While until a few years ago, it was impossible to speak of diversification within a cryptocurrency portfolio because they all merely amplified the performance of Bitcoin. Today, the investor has more freedom of movement, as the dominance is between 40 and 50 percent. Now, for every dollar that enters the cryptocurrency market, only 50 cents are invested in Bitcoin. In all likelihood, the correlation will vanish almost

completely when (and if) dominance drops below 20 percent.

Therefore, it is clear how foolish it is today to create a portfolio with 100 different cryptocurrencies and think of it as diversification. In fact, by doing so, you are increasing your financial risk as you are essentially buying an amplification of Bitcoin's movements.

Still acting as a market index, it can only make sense to invest in other cryptocurrencies if:

- they are at least somewhat untethered from Bitcoin;
- they offer a higher return potential.

As we will see later, there are very few projects that meet these characteristics.

Furthermore, as we look at other factors related to investing in cryptocurrencies, the list of these criteria will be updated. At the end of the book, you will find a complete checklist of a cryptocurrency's characteristics to be considered a good investment.

The value of dominance can be checked on a site that every cryptocurrency investor should know about. We have also discussed in the more theoretical books: CoinMarketCap (coinmarketcap.com).

Before proceeding further, let us make an important point clear: there is nothing wrong with investing only in Bitcoin without buying other cryptocurrencies; buying other projects does not reduce financial risk.

To recap

- Bitcoin's dominance directly indicates how much Bitcoin's capitalization weighs on the total market.

PART 6 - ECONOMIC ANALYSIS OF CRYPTOCURRENC

Chapter 23 - The Capitalization of Cryptocurrencies

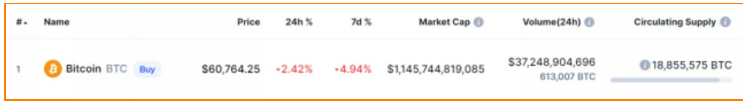
Using the data provided by CoinMarketCap, you can get an idea of the internal economics of a cryptocurrency. This is crucial to understand what you are investing in and assess whether or not it makes sense to include that asset in your portfolio. So let's start by understanding what data can help us in this task.

Capitalization

We have already mentioned this concept in the previous chapters. Capitalization, in general terms, indicates the total amount of money present in an asset. Its value is given by multiplying the number of units in circulation by the unit price.

For example, the capitalization of the Apple

brand is the multiplication of the number of shares on the market by the price of a single claim. Similarly, the capitalization of Bitcoin is given by the product of the number of Bitcoins in circulation and the cost of one BTC.



#↓	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
1	Bitcoin BTC Buy	$60,764.25	-2.42%	-4.94%	$1,145,744,819,085	$37,248,904,696 613,007 BTC	18,855,575 BTC

As you can see from the image, multiplying 39,215.42 dollar by 18,787,925 BTC gives exactly 735 billion dollar in capitalization. Does this mean that there is all this money invested in the Bitcoin ecosystem? The reality is a bit more complex than it seems. Capitalization is a 'derivative,' i.e., a value obtained from a mathematical operation of other data. Therefore, it does not give us weighted information about a fact but is a hypothesis that tries to associate a number with the total value.

To better understand the concept, here is an example. Let's assume that there are the same bitcoins in circulation as there are now, so 18,787,925 and that, to date, there has never been a bitcoin trade. Therefore, since the last

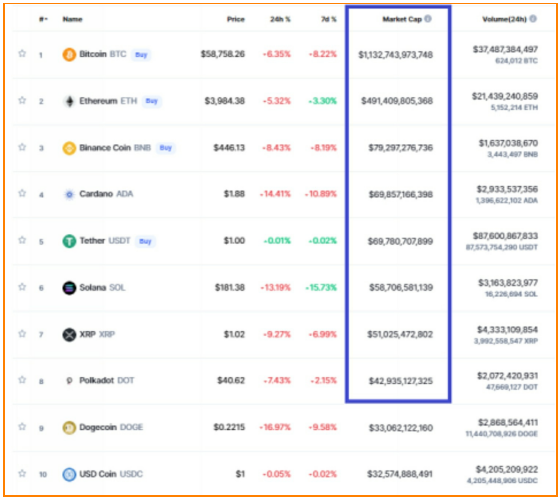
recorded price is 0 dollar, the capitalisation will be: 18,787,925 x 0 = 0 dollar. Let us now assume that Marie wants to buy one bitcoin from James for 1 dollar. Following this transaction, the last recorded price would be one dollar per bitcoin. The new capitalisation of bitcoin would now be 18,787,925 x 1 = 18,787,925 dollar. As you can see, the asset would have reached a billion-dollar valuation with only one dollar of actual transactions.

So, where does the usefulness of capitalization lie? Well, it lies in the possibility of using it as a method of comparison between different cryptocurrencies. The cryptocurrency investor can use this data to understand which of two or more assets is valued more by the market. In particular, this can be highly convenient in the case of two cryptocurrencies with comparable prices.

To understand better, let us compare Bitcoin with Yearn Finance in this case. As can be seen, the YFI token is priced similarly to BTC.

This might lead the unwary investor to think that the value of the two coins is also the same. However, if we compare the capitalizations, we quickly understand that Bitcoin is about 500 times "bigger" than Yearn Finance. In fact, to have the same capitalization, a YFI would have to be worth over 20 million dollar s.

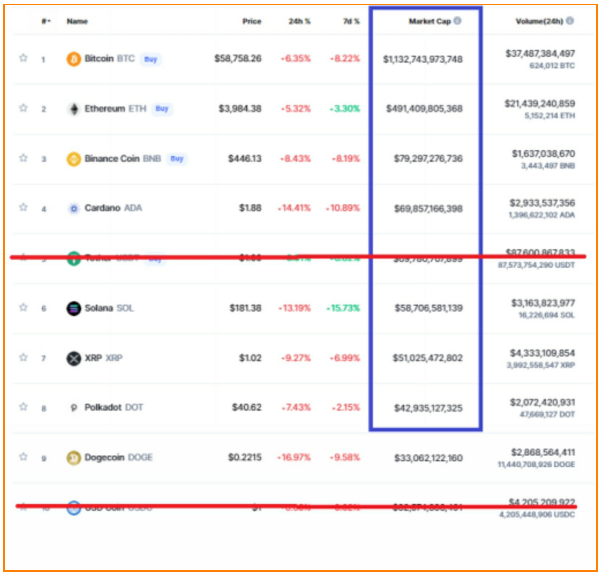
The advice for those approaching cryptocurrencies for the first time is not to invest, with a few rare exceptions, in assets that do not have at least $40 billion in capitalization. Analyzing the data provided by CoinMarketCap, this criterion reduces the number of existing cryptocurrencies from over 11,000 to around ten (in the grid below, you will see 9 of them highlighted).



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)
1	Bitcoin BTC Buy	$58,758.26	-6.35%	-8.22%	$1,132,743,973,748	$37,487,384,497 624,012 BTC
2	Ethereum ETH Buy	$3,984.38	-5.32%	-3.30%	$491,409,805,368	$21,439,240,859 5,152,214 ETH
3	Binance Coin BNB Buy	$446.13	-8.43%	-8.19%	$79,297,276,736	$1,637,038,670 3,443,497 BNB
4	Cardano ADA	$1.88	-14.41%	-10.89%	$69,857,166,398	$2,933,537,356 1,396,622,102 ADA
5	Tether USDT Buy	$1.00	-0.01%	-0.02%	$69,780,707,899	$87,600,867,833 87,573,754,290 USDT
6	Solana SOL	$181.38	-13.19%	-15.73%	$58,706,581,139	$3,163,823,977 16,226,694 SOL
7	XRP XRP	$1.02	-9.27%	-6.99%	$51,025,472,802	$4,333,109,854 3,992,558,547 XRP
8	Polkadot DOT	$40.62	-7.43%	-2.15%	$42,935,127,325	$2,072,420,931 47,669,127 DOT
9	Dogecoin DOGE	$0.2215	-16.97%	-9.58%	$33,062,122,160	$2,868,564,411 11,440,708,926 DOGE
10	USD Coin USDC	$1	-0.05%	-0.02%	$32,574,888,491	$4,205,209,922 4,205,448,906 USDC

Furthermore, stablecoins must be excluded from the list. In our academic books, we have dealt technically with what they are and how they are programmed. In this instance, we will repeat that they are cryptocurrencies whose value remains stable over time. As a result, they do not offer any capital appreciation possibilities and should not be considered among the choices. In the list above, the stablecoins presents are USDT and USDC.

That being said, let’s now actually remove stablecoins from the aforementioned list; that would now leave us with 7 options.



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)
1	Bitcoin BTC Buy	$58,758.26	-6.35%	-8.22%	$1,132,743,973,748	$37,487,384,497 624,012 BTC
2	Ethereum ETH Buy	$3,984.38	-5.32%	-3.30%	$491,409,805,368	$21,439,240,859 5,152,214 ETH
3	Binance Coin BNB Buy	$446.13	-8.43%	-8.19%	$79,297,276,736	$1,637,038,670 3,443,497 BNB
4	Cardano ADA	$1.88	-14.41%	-10.89%	$69,857,166,398	$2,933,537,356 1,396,622,102 ADA
5	Tether USDT Buy	$1.00	0.01%	0.02%	$69,782,767,899	$87,600,867,833 87,573,754,290 USDT
6	Solana SOL	$181.38	-13.19%	-15.73%	$58,706,581,139	$3,163,823,977 16,226,694 SOL
7	XRP XRP	$1.02	-9.27%	-6.99%	$51,025,472,802	$4,333,109,854 3,992,558,547 XRP
8	Polkadot DOT	$40.62	-7.43%	-2.15%	$42,935,127,325	$2,072,420,931 47,669,127 DOT
9	Dogecoin DOGE	$0.2215	-16.97%	-9.58%	$33,062,122,160	$2,868,564,411 11,440,708,926 DOGE
10	USD Coin USDC	$1	0.04%	0.02%	$32,874,388,161	$4,205,209,922 4,205,448,906 USDC

You may now begin to understand the reasoning behind this seemingly peculiar way of investing. It's not about buying projects with the hope of them overtaking Bitcoin, but about only putting cryptocurrencies in your portfolio that can offer asymmetric returns compared to BTC while not exponentially raising your financial risk.

We, therefore, update the list of criteria that a cryptocurrency must meet to be attractive as an investment. It must:

- Be relatively unrelated to Bitcoin;

- Offer a higher return potential;
- Have a minimum capitalization of $40 billion;
- Not be a stablecoin.

To recap

- Capitalization indicates how "big" a cryptocurrency is.
- Some cryptocurrencies are created with vast circulations of cash to make them seem cheap.
- The price of a cryptocurrency tells us little or nothing if not compared to its capitalization.
- Stablecoins are cryptocurrencies that maintain a constant value.

Chapter 24 - The Inflation Rate

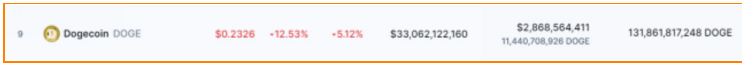
Inflation can be defined in two ways:

- The reduction in the purchasing power of a given currency
- The sustained increase in the price of goods and services in an economy.

While in traditional finance, inflation is caused by the monetary input of central banks, in cryptocurrencies, it is caused by the number of coins put on the market following the validation of a blockchain. Once again, we have discussed this topic in-depth in our academic books. Here, we shall mention that every cryptocurrency, in one way or another, gives a reward to those who validate transactions onto the network. This is not only an economic incentive but also how new coins are introduced into the system. Since the meeting of supply and demand gives the price, cryptocurrencies with many coins in circulation or with a very high monetary

input will find it difficult to sustain their price and thus bring good returns to investors.

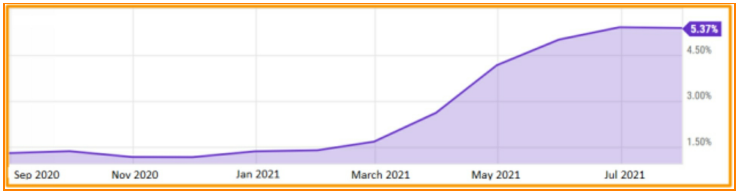
Listed in the previous chapter, the most inflationary coin is Dogecoin, with an addition of 30,000 DOGE every minute. This is also reflected in the total amount in circulation, which, as you can see, is over 130 billion.



Bitcoin, on the other hand, has a built-in progressive deflationary system. This means that the more time passes, the fewer BTCs are put on the market. This is made possible by a phenomenon called "halving," which halves the premium given to transaction validators, the miners, about every four years. Add to this the fact that the maximum number of bitcoins that will ever be available is 21 million. So it is understandable why many investors consider BTC to be a good asset against the inflation of legal tender currencies. Let's go into a little more detail.

Over the past year, US dollar inflation has reached 5.37%. This means that if an

American has not increased their assets by 5.37% over the past year, they will have lost some purchasing power.



In 2020, Bitcoin saw its fourth halving, which halved its inflation and brought the premium for miners from 12.5 BTC to 6.25 BTC per block. Recall that a block on Bitcoin is validated every 10 minutes. As a result, anyone who has held this asset for more than a year has doubled their spending power in terms of BTC. In dollar terms, this has also led to an increase in bitcoin price from $11,581 to around $50,000 per BTC.

Bitcoin, therefore, structurally contrasts with

the dollar and other legal tender currencies precisely because of its deflation and planned scarcity. While no one can know what the economic policies of Europe and America will be, Bitcoin's economy is public and known to all. This same transparency makes it, according to many investors, an excellent asset against ECB and FED monetary expansion. Logically, it is best to avoid any cryptocurrency with higher domestic inflation than the legal tender currency you are using as a reference.

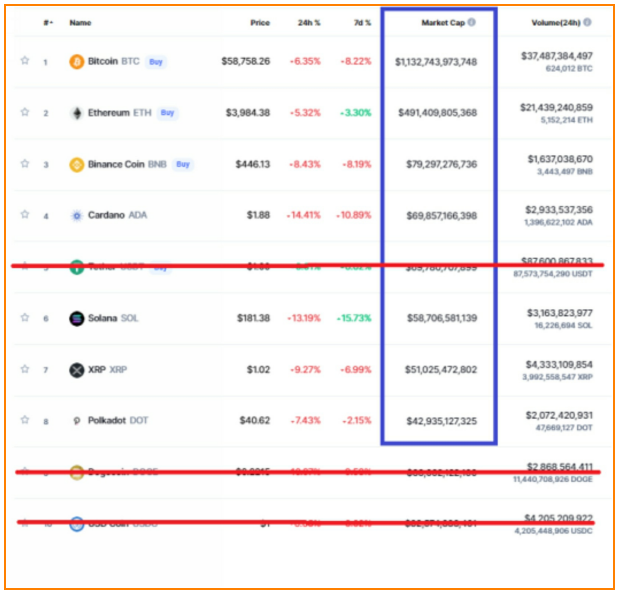
Low inflation does not necessarily mean good investments

While a cryptocurrency with a high domestic inflation rate is almost always ill-advised, the opposite is invalid. To ride the market euphoria, fraudsters often create currencies with negative inflation to attract incompetent investors. In 100% of these cases, the scam ends with the cryptocurrency developers

selling off the cryptocurrency on a massive scale, driving the price close to zero and leaving the buyers with nothing.

But how to recognize these scams? The list of characteristics we have already mentioned a couple of times is a good starting point. To this, we can add an important criterion. If the project has the sole purpose of being deflationary, then it is better to stay away from it. A classic example of this approach is the SAFEMOON token, whose economic structure is built exclusively to sell the coin disadvantageous. Even in this case, holders have to pay a 10% commission to get rid of the cryptocurrency. Typically, the market itself makes the life of these 'projects' short, but in times of extreme euphoria, some novices can get trapped and lose their capital.

Low inflation, therefore, is a necessary but not sufficient condition to make a cryptocurrency a viable investment vehicle. We can consequently exclude DOGE from the list; However, many love it for its playful nature. It is not suitable for a serious investor.



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)
1	Bitcoin BTC Buy	$58,758.26	-6.35%	-8.22%	$1,132,743,973,748	$37,487,384,497 624,012 BTC
2	Ethereum ETH Buy	$3,984.38	-5.32%	-3.30%	$491,409,805,368	$21,439,240,859 5,152,214 ETH
3	Binance Coin BNB Buy	$446.13	-8.43%	-8.19%	$79,297,276,736	$1,637,038,670 3,443,497 BNB
4	Cardano ADA	$1.88	-14.41%	-10.89%	$69,857,166,398	$2,933,537,356 1,396,622,102 ADA
5	Tether USDT Buy	$1.00	0.01%	0.02%	$65,780,707,895	$87,600,867,833 87,573,754,290 USDT
6	Solana SOL	$181.38	-13.19%	-15.73%	$58,706,581,139	$3,163,823,977 16,226,694 SOL
7	XRP XRP	$1.02	-9.27%	-6.99%	$51,025,472,802	$4,333,109,854 3,992,558,547 XRP
8	Polkadot DOT	$40.62	-7.43%	-2.15%	$42,935,127,325	$2,072,420,931 47,669,127 DOT
9	Dogecoin DOGE	$0.2515	-10.07%	-9.69%	$33,002,152,153	$2,868,564,411 11,440,708,926 DOGE
10	USD Coin USDC	$1	0.00%	0.00%	$32,971,650,191	$4,205,209,922 4,205,448,906 USDC

The field gets narrower and narrower. Once again, it is necessary to observe how one proceeds methodically without getting caught up in emotions. This is undoubtedly an essential skill for those who want to invest successfully.

Let's further update the list of criteria that a cryptocurrency must meet to be attractive as an investment:

- It must be relatively unrelated to Bitcoin;
- It must offer a higher return potential;

- It must have a minimum capitalization of $40 billion;
- It must not be a stablecoin;
- It must have lower domestic inflation than the investor's reference legal tender currency;
- It must not make deflation its sole strength.

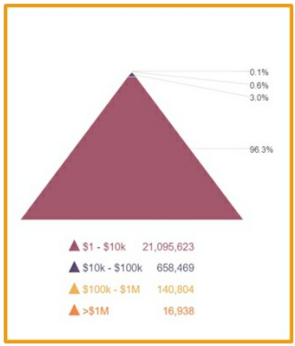
As we can see, adding these criteria to the list removed another option, leaving us with 6.

To recap

- In a scenario where inflation is over 5%, those who do not invest constantly lose purchasing power.
- One should stay away from cryptocurrencies that have higher domestic inflation than the inflation rate of the legal reference tender.
- A low inflation rate does not always coincide with a good investment.

Chapter 25 - Wealth Distribution

The third fundamental aspect of being considered while analyzing and understanding if it's possible to invest without exposing oneself to excessive financial risk is the distribution of wealth.
Thanks to the fact that blockchains are public, it is possible to see if, in any given project, there are concentrations of wealth that could make it unsafe or subject to unexpected massive sales. Let us take the case of Bitcoin as an example.



In this case, it is evident that most of the value is held by most people: this is good, as

a handful of entities can't manipulate the price into rising or dropping with ease. This results in greater security for the investor and a healthier and more sustainable financial system.

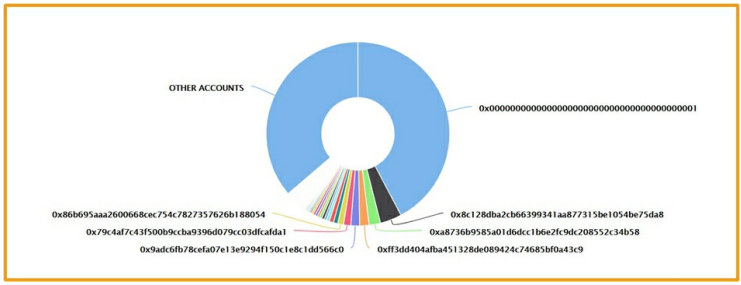
In the top 10 by capitalization, some cryptocurrencies do not reflect this parameter. In particular, Ripple and its XRP token are controlled by very few users. According to the website Ledger Exposed (ledger.exposed/rich-stats), 64% of the XRP in circulation is held by just 100 entities. This allows these 100 large investors to "play" with the token's price without ever losing control.

Having to define a numerical parameter, we can say that if 50% of the circulating amount is not distributed among at least 50% of the holders, it is better not to invest in that cryptocurrency.

In the top 10 in terms of capitalization, XRP and SOL can be excluded as investment vehicles, with 70% of the circulating capital held by 0.04% of the users.

#▪	Name	Price	24h %	7d %	Market Cap	Volume(24h)
1	Bitcoin BTC Buy	$58,758.26	-6.35%	-8.22%	$1,132,743,973,748	$37,487,384,497 624,012 BTC
2	Ethereum ETH Buy	$3,984.38	-5.32%	-3.30%	$491,409,805,368	$21,439,240,859 5,152,214 ETH
3	Binance Coin BNB Buy	$446.13	-8.43%	-8.19%	$79,297,276,736	$1,637,038,670 3,443,497 BNB
4	Cardano ADA	$1.88	-14.41%	-10.89%	$69,857,166,398	$2,933,537,356 1,396,622,102 ADA
[redacted]						$87,600,867,833 87,573,754,290 USDT
[redacted]						$3,163,823,977 16,226,694 SOL
[redacted]						$4,333,109,854 3,992,558,547 XRP
8	Polkadot DOT	$40.62	-7.43%	-2.15%	$42,935,127,325	$2,072,420,931 47,669,127 DOT
[redacted]						$2,868,564,411 11,440,708,926 DOGE
[redacted]						$4,205,209,922 4,205,448,906 USDC

Having a high concentration of wealth in the hands of very few people is often indicative of a scam, especially when combined with marked deflation and disincentives to sell. Since we mentioned SAFEMOON earlier, let us study its distribution.



It can be seen that more than half of the coins are held by only seven addresses. SAFEMOON LLC, the company behind this project, has stated that the address 0x000000000000000000000000000000000000 is used to take the tokens out of the market (again leveraging deflation) and that it will never be used for outward transactions. However, there is no certainty that this is true and that these funds will not be moved in the future to be sold on the market. Therefore, if it's required to trust a third-party entity, this is not a good investment in the cryptocurrency sector.

Two critical points are added to our list. For a cryptocurrency to be a good investment:

- It must be relatively untethered from Bitcoin;
- It must offer a higher return potential;
- It must have at least a capitalization of 40 billion dollars;
- It must not be a stablecoin;
- It must have lower domestic inflation than the investor's reference legal tender

currency;

- It must not make deflation its sole strength;
- It must have 50% of the cash distributed among at least 50% of the investors;
- It must not require trust in an external company or entity.

Each chapter makes it clearer how to navigate this sector, and chance is shown less sDCAe. So let's get on with it! All this being said, we are left with five projects still to consider.

To recap

- You should avoid buying cryptocurrencies that have most of the wealth stored in a small number of addresses.
- Bitcoin has a fairer distribution of wealth than legal tender currencies.

Chapter 26 - The Longevity of a Cryptocurrency

Longevity is the most challenging parameter to define and requires some "eye" on the part of the investor. It is a sensitivity that can only be acquired with time and cannot be reduced to a numerical parameter. In this chapter, we will, however, do our utmost to eliminate the need for intuition.

Longevity indicates how long a cryptocurrency has been on the market and, more importantly, how long it expects to stay there.

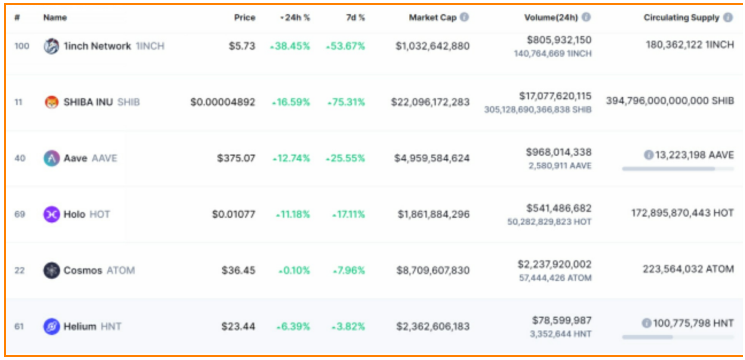
Thanks to CoinMarketCap, we can analyze the historical data of this market. On 31 December 2017, this was the top 10 by capitalization.

Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$237,466,518,547.07	$14,156.44	16,774,450 BTC	$12,136,306,688.00	0,01%	8,41%	4,21%
2	XRP	XRP	$89,121,967,114.06	$2.30	38,739,144,847 XRP *	$4,642,084,864.00	0,18%	5,75%	125,31%
3	Ethereum	ETH	$73,170,132,771.99	$756.73	96,692,190 ETH	$2,554,265,856.00	0,30%	4,91%	8,78%
4	Bitcoin Cash	BCH	$42,774,236,530.93	$2,533.01	16,886,713 BCH	$1,300,817,280.00	-0,43%	5,00%	-9,87%
5	Cardano	ADA	$18,659,588,487.38	$0.7197	25,927,070,538 ADA	$305,947,200.00	-0,82%	6,15%	91,25%
6	Litecoin	LTC	$12,663,197,417.17	$232.10	54,560,158 LTC	$771,042,368.00	-0,75%	5,27%	-14,18%
7	IOTA	MIOTA	$9,869,763,787.81	$3.55	2,779,530,283 MIOTA *	$167,521,280.00	-0,27%	5,03%	5,77%
8	NEM	XEM	$9,306,424,139.90	$1.03	8,999,999,999 XEM *	$69,870,056.00	1,82%	10,48%	6,45%
9	Dash	DASH	$8,189,388,164.00	$1,051.68	7,786,970 DASH	$154,690,112.00	-0,98%	4,05%	-9,85%
10	Stellar	XLM	$6,442,724,493.37	$0.3608	17,858,965,917 XLM *	$183,768,320.00	1,19%	10,47%	66,56%

It can be seen that only five of the cryptocurrencies that were at the top of the list at the time are still relevant today. Indeed, these projects have stood the test of time and a bear market of over three years makes them much more attractive to an investor today.

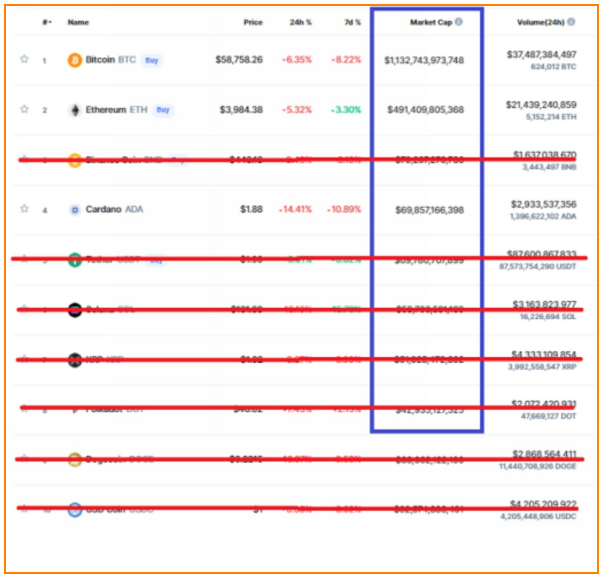
So does this mean that any cryptocurrency that hasn't been around for at least three years is not a good deal? In absolute terms, no. For the investor profiled at the beginning of the book, however, a too recent project is not suitable for long-term investment, as it lacks certain historicity that suggests a bright future. Nevertheless, in the short term and for more speculative operations instead, these "minor" tokens can be real gems. In fact, over the last 7 days, it can be observed that the projects that have had the most significant returns do not even remotely belong to the

top 10 most capitalized.



#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
100	1inch Network 1INCH	$5.73	-38.45%	-53.67%	$1,032,642,880	$805,932,150 140,764,669 1INCH	180,362,122 1INCH
11	SHIBA INU SHIB	$0.00004892	-16.59%	-75.31%	$22,096,172,283	$17,077,620,115 305,128,690,366,838 SHIB	394,796,000,000,000 SHIB
40	Aave AAVE	$375.07	-12.74%	-25.55%	$4,959,584,624	$968,014,338 2,580,911 AAVE	13,223,198 AAVE
69	Holo HOT	$0.01077	-11.18%	-17.11%	$1,861,884,296	$541,486,682 50,282,829,823 HOT	172,895,870,443 HOT
22	Cosmos ATOM	$36.45	-0.10%	-7.96%	$8,709,607,830	$2,237,920,002 57,444,426 ATOM	223,564,032 ATOM
61	Helium HNT	$23.44	-6.39%	-3.82%	$2,362,606,183	$78,599,987 3,352,644 HNT	100,775,798 HNT

Following the addition of this parameter, we must also remove Polkadot (DOT) and Binance Coin (BNB) from the possible choices. So from over 11,000 different cryptocurrencies, we have concluded that only 3 of them fit the profile of our investor.



Let's add, then, the last parameter for evaluating a cryptocurrency. To be a good investment a currency:

- It must be relatively untethered from Bitcoin;
- It must offer a higher return potential;
- It must have at least a capitalization of 40 billion dollar;
- It must not be a stablecoin;
- It must have lower domestic inflation than the investor's reference legal tender

currency;

- It must not make deflation its sole strength;
- It must have 50% of the cash distributed among at least 50% of the investors;
- It doesn't require reliance on an external company or entity;
- It must have been on the market for at least three years and have survived a bear market.

Please note that at the end of this book, you will find a handy checklist with these points so that in the future, you can analyze at a glance the cryptocurrencies that interest you most.

To recap

- There is no mathematical criterion for the longevity of a cryptocurrency.
- It tends to be better to prefer projects that

have been around for at least three years and have survived a bear market.

- You should not "invest" in cryptocurrencies simply because they are fashionable.

PART 7 - BUYING, SELLING AND STORING CRYPTOCURRENC

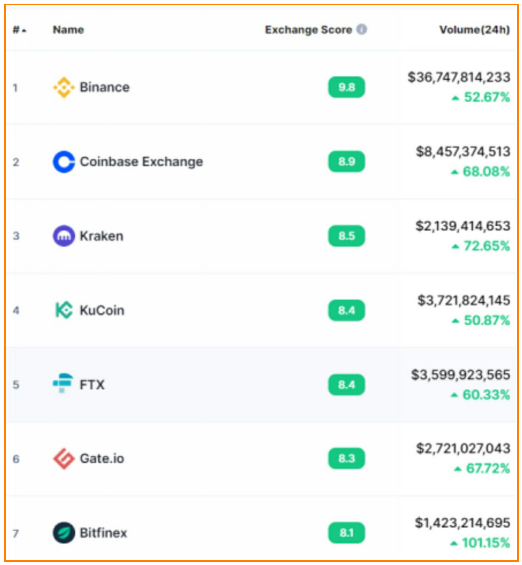
Chapter 27 - Choosing an Exchange

To buy and sell cryptocurrencies, you need to use an exchange. You can think of it as a sort of broker dedicated exclusively to this specific market. The most famous ones internationally are certainly Coinbase (coinbase.com) and Binance (binance.com).

The former is famous for its user-friendly graphics. At the same time, the latter is known in the industry for many cryptocurrencies it allows you to buy. Considering that the investor profiled at the beginning of this book does not need to make any purchases, as they will operate long-term, no exchange is markedly more appropriate than another. There are, however, also in this case, parameters that can be useful to avoid operating through little questionable societies that perhaps attract the most inexperienced investors with of their "promotions."

Firstly, it is necessary to consider the identity verification that the exchange carries out on its users. In fact, according to European rules, every financial intermediary is required to collect information about its customers. As annoying as it can be to send a copy of your driving license and wait for identity verification, this is a fundamental step to be protected if something goes wrong. It would help if you always were wary of exchanges that allow you to buy and sell cryptocurrencies without providing your details.

Once again, CoinMarketCap comes in handy to get an idea of which solutions are best. It can be seen that Binance and Coinbase are the two exchanges with the highest volumes. This means that many users choose them to carry out their transactions.



#	Name	Exchange Score	Volume(24h)
1	Binance	9.8	$36,747,814,233 ▲ 52.67%
2	Coinbase Exchange	8.9	$8,457,374,513 ▲ 68.08%
3	Kraken	8.5	$2,139,414,653 ▲ 72.65%
4	KuCoin	8.4	$3,721,824,145 ▲ 50.87%
5	FTX	8.4	$3,599,923,565 ▲ 60.33%
6	Gate.io	8.3	$2,721,027,043 ▲ 67.72%
7	Bitfinex	8.1	$1,423,214,695 ▲ 101.15%

Another parameter to consider is the fiscal and legal location of the exchange. A good practice is to only operate with intermediaries located in states that are deemed low-risk by the authorities in your country of residence.
For example, Coinbase is based in America. Binance, on the contrary, is based in Cyprus, a country not well-loved by the US when it comes to financing. Therefore, it is advisable to choose an exchange such as Coinbase or Kraken, based in Canada, the US, and the UK.

However, this can and will only be a rough

guide to help you choose the exchange you feel most comfortable with. As we will later see, cryptocurrencies will be moved to a wallet that is disconnected from any intermediary. From that point on, the choice of exchange used will take a back seat.

This book will not go through the step-by-step process of buying and selling cryptocurrencies on these exchanges. This is for two reasons:

- The reader of this book is undoubtedly familiar enough with the technology to figure out "where to click" on their own;
- As these are websites anyway, the layout of the buttons can change from one day to the next, and you want to avoid this book becoming obsolete before it is even published.

To recap

- Cryptocurrencies are bought on platforms called exchanges.
- It would be best to only use high-volume

exchanges that have been around for several years.

- The best international solutions are Coinbase and Binance.

Chapter 28 – Storing your Crypto

This is a crucial chapter, as many people interested in cryptocurrencies do not invest for fear of 'losing their money' to fraudulent third parties running off with their users' coins. This is a legitimate concern, but it is a shame to see how this negative outlook is not counterbalanced by looking at the solutions to prevent this from happening. Because there are indeed systems in place to ensure the total security of one's cryptocurrencies, and on these pages, we will find out what they are.

As mentioned above, it is unwise for the long-term investor to hold their funds on any exchange. The advantage of cryptocurrencies is that they allow the owner to hold them themselves without trusting and relying on intermediaries.

In the past, there have been cases of significant hacker attacks in this sector, which have caused the total loss of many

people's investments. The most famous of all is undoubtedly the Mt.Gox hack, which took place in 2014. Hackers exploited a weakness in the exchange's security system. As a result, they managed to get hold of more than 700,000 bitcoins, which at the time were worth around $400 million. This was a massive blow to the entire industry, as Mt.Gox was the equivalent of what Coinbase and Binance are today. For all cryptocurrency investors, it was a warning to store their cryptocurrencies independently, leaving them on the exchange just long enough to buy and sell.

But then, where should one's coins be kept? The answer is simple: in a cryptocurrency wallet.

Unlike a regular wallet, which may contain banknotes and physical coins, cryptocurrency wallets do not hold funds. Cryptocurrencies are always on the blockchain but can only be accessed using an alphanumeric string called a private key. Private keys prove an investor's ownership of a certain amount of coins and allow them to access and mobilize the tokens.

If you lose your private keys, you automatically lose access to your funds. This is the risk associated with the great freedom of being 100% owner and controller of your money. If you lose access, there is no external entity to help you.

Wallets range from simple-to-use apps to more complex security solutions. The main types of wallets to choose from are as follows.

Paper wallet:

Private keys are written on a physical medium such as paper and stored in a secure location. This makes cryptocurrencies more difficult, as the paper wallet does not give direct access to the network. Those who use this solution are investors who have no interest in touching their tokens for several years.

Hardware wallet:

Private keys are stored in a device that is kept in a safe place and connected to a computer only when a transaction is to be made. The

idea is to balance the security of a paper wallet with an ease of use that allows quick mobilization of funds.

Online wallet:

Private keys are stored in an application or other software. This makes sending, receiving, and using cryptocurrencies very similar to using any home banking system. However, there is some loss of security here, as the wallet is always connected to the internet and can be subject to hacking attacks.

The best solution for the investor profiled at the beginning of this book is to use a hardware wallet. The two most important companies producing this type of wallet are Trezor (trezor.io) and Ledger (ledger.com). Both are a good choice and offer a very high degree of protection, suitable for long-term investments. Suppose you have large amounts of cryptocurrency to manage. In that case, it is a good idea to split the funds into several wallets to diversify and limit the risk associated with managing your money independently.

Again, since the 'where to click' is very intuitive and the graphical interface can change from one moment to the next, it is preferable not to include a written tutorial to avoid rapid obsolescence of the information shared.

To recap

- After buying cryptocurrencies, you should transfer them to your wallet.
- A wallet is a tool that holds the private keys of an address.
- There are network wallets and hardware wallets.
- Networked wallets are more user-friendly but less secure.
- Hardware wallets are more complex to use but offer better security.

PART 8 - INVESTMENT STRATEGY

Chapter 29 - Capital Allocation

To create and evaluate an investment strategy, it is necessary to understand its purpose and potential returns. In our case, after a great deal of selection work in the previous chapters, we have concluded that the choice can fall between three cryptocurrencies for the investor profiled at the beginning of the book.

Beforehand one cannot say whether it might be a good idea to invest in all three and in what proportion. To add this piece of information, it is necessary to understand the objective of the investment. Let us recall the characteristics of our investor:

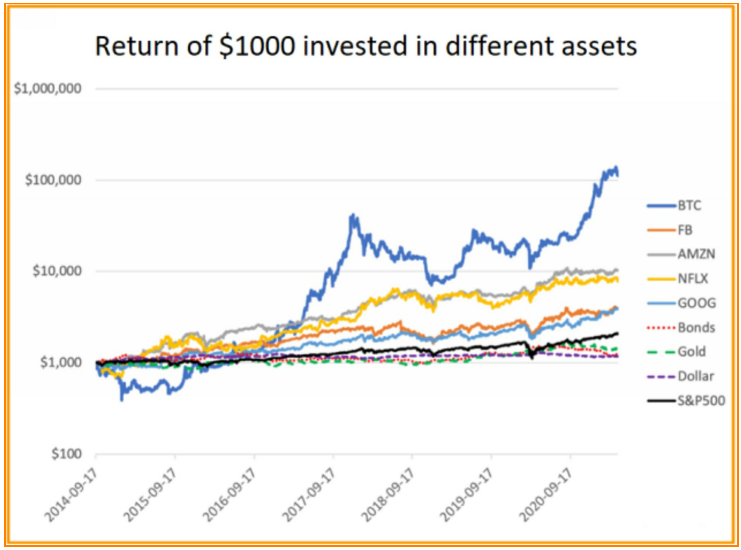
- They have a steady income that allows them to have a surplus of money at the end of the month;
- They have a liquid emergency fund equal to at least six months of their lifestyle;
- Wants to invest for the long term.

Let's now see how these factors affect capital allocation.

Investing for the long term

Suppose you have to invest for the long term. In that case, most of your capital should be allocated to the cryptocurrency that has managed to deliver the most consistent results over time. Well, of the three, Bitcoin is the one that best meets this yardstick. The chart below compares the performance of a $1000

investment from 2014 to 2017 on some of the most common assets with that of bitcoin.



It can be seen that the trend is quite similar in terms of "charts," but also that Bitcoin has amplified its returns compared to other assets. This means that the most capitalized cryptocurrency is, to date, reasonably correlated with the rest of the market but tends to offer higher returns. In particular, while the S&P 500 has appreciated by an average of 14% per year over the past ten years, BTC has risen by around 200% annually.

Investing regularly

Another important aspect for our investors to consider is that they have a relatively constant income each month, which allows them to have a recurring amount of capital to invest. As a result, we can add another piece to the strategy we are building: there will not be one significant initial investment, but we will build up positions consistently and enter the market. In other words, we will make a dollar-cost averaging plan, also known as DCA

In this case, this is a forced choice, but is it also an excellent way to invest in cryptocurrencies? The next chapter answers this question.

To recap

- When investing, it is best to do so for the long term.
- The S&P 500 has returned 14% annually over the past ten years, while BTC has grown by 200% each year.

- A dollar-cost averaging is the most common choice for long-term investing.

Chapter 30 – The Dollar Cost Averaging Plan (DCA)

The dollar-cost averaging plan is an investment strategy that aims to reduce the imDCAt of the volatility of an asset. It involves the purchase of equal amounts of the asset at regular intervals of time.

For example, the investor taken as a model for this book can invest once a month, thanks to the surplus given by their salary.

The theoretical premise of the dollar-cost averaging plan is that by entering the market in this way, the investment can reduce the fluctuations that there would be if one were to immediately invest the entire sum one wishes to devote to that asset. In the long run, such a strategy reduces the negative imDCAt that entering the market at the wrong time can have on the investment.

Why make a dollar-cost averaging plan

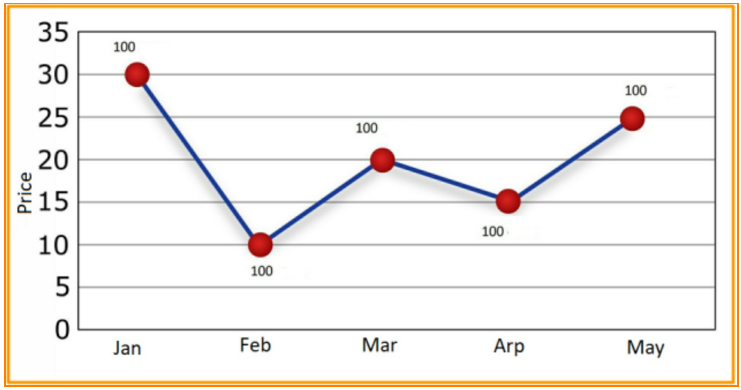
Many dollar-cost averaging plan s profess the main advantage of reducing the risk of investing at the wrong time for the market. Suppose you divide your investment into smaller chunks. In that case, one thinks they can achieve better results than if they invested all their capital at once. As we will see in a moment, however, this is only true for some specific assets.

In any case, the dollar-cost averaging plan does not entirely mitigate financial risk. The idea is to facilitate market entry to minimize the risk of bad timing. Here is how it works.

An example of a dollar-cost averaging plan

Suppose you have a fixed amount of $500 to invest in Bitcoin. The dollar-cost averaging plan, in this case, is to divide the 500 dollar into five parts of 100 dollar each. Every

month, we will buy 100 dollars worth of Bitcoin, regardless of the price. In this way, we will extend our entry to a period of five months. Our entry price will be exactly the average price of the last five months, as the capital has been divided into equal parts. The following image shows this concept graphically.

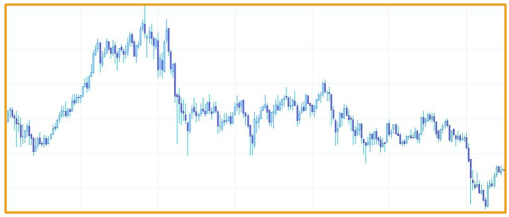


For which assets should a dollar cost average be used?

For many investors, the dollar-cost averaging plan is the panacea for all ills. After all, they are under the impression that by staggering their income, they can achieve an average

entry price that is always better than if they invested all their capital at the same time. This, however, is only true for assets that do not have a bullish trajectory over the long term.

For example, we take the monthly diagram of the price of the ENI stcok from 2002 until today.



As can be seen, the trajectory over more than 19 years is not at all bullish. In this case and similar situations, averaging the price may make sense because it allows you to buy the asset at a statistically more practical level than investing in a lump sum. However, the same cannot be said for all those financial instruments that tend to rise steadily over time. An example outside of the cryptocurrency sector is the S&P 500, which on average, has seen an appreciation of 12% per year. As you can see, looking at a period

of 19 years, the trend is consistently bullish.

In such circumstances, the time during which one is invested matters more than the entry price. This is because the asset will tend to cost more tomorrow than today, so there is no point in waiting or delaying entry.

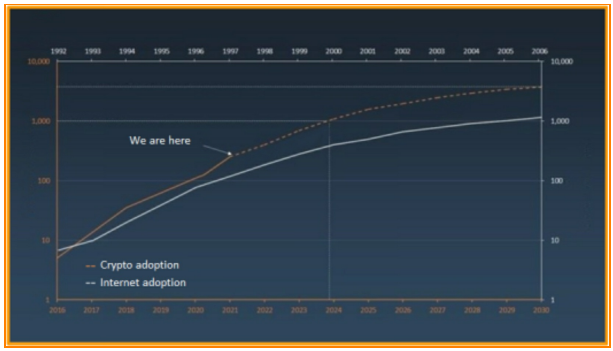
Bitcoin also falls into the same category as the S&P 500. Its chart speaks very clearly and shows an apparent upward propensity.

It follows that, in economic terms, it is much better to invest all the capital as soon as possible, rather than to enter in stages. However, as mentioned, this is not possible for our model investors, and they will have to

"make do" with a monthly dollar-cost averaging plan. Nevertheless, it is good to know that this is not the most profitable choice, so don't be afraid to invest sudden capital surpluses given the eventualities of life; if one month the 20% of the capital to be allocated to investments (remember that we said that our model investor could have up to 20% of his assets in cryptocurrencies) is 150 dollar compared to an average of 100 dollar, it doesn't make sense to wait to invest that extra 50 dollar. Mathematically, they will give a higher return if they are put on the market immediately.

The same applies to ETH and ADA, which, as mentioned, are not wholly unrelated to Bitcoin.

Even on a purely fundamental level, if you look at the blockchain as a technology and observe its adoption curve, you can see that it makes no sense to defer your income when you don't need to.



At this point, the investor might ask themselves whether it is possible to do something to get closer to the returns from investing all the capital in one go while being forced to rely on a dollar-cost averaging plan. The answer is yes.

To recap

- The dollar-cost averaging plan consists of investing the same amount every month.
- It is a strategy that works very well for assets that are not growing steadily.
- It is not the best way to invest in cryptocurrencies.

Chapter 31 - The Advanced Dollar-Cost Averaging Plan (ADCA)

This is the strategy that, statistically, allows you to invest in cryptocurrencies with staggered income over time while equally approaching (and sometimes even exceeding) the performance of investing in one lump sum. This claim is supported by data, which will be shown shortly.

To fully understand it, however, it is necessary to introduce and understand the concept of the simple moving average, which is fundamental to this investment technique.

The simple moving average

The simple moving average computes data from a specific period. It produces the average price of the asset for that period. The difference between a simple moving average

and a mathematical average of past prices is that the simple moving average eliminates older data as new data is added. For example, suppose the simple moving average calculates the average price over 50 days. In that case, the information is constantly updated as time goes on to take into account only the last 50 days.

It is important to note that all data in a simple moving average are weighted in the same way, regardless of how recent they are. This means that the price from 50 days ago has the same importance as the current price when calculating the average.

This is what the 50-period simple moving average looks like on the Bitcoin chart.

As can be seen, the orange line (which is the simple moving average) follows the Bitcoin

price trend, but more smoothly, reducing the 'noise' from upward or downward excesses. Since simple moving averages use past prices rather than current prices, they have a certain lag period. The larger the data period considered, the more significant the lag.

For example, a moving average that looks at the last 200 days will respond more slowly to new information than a simple moving average that only looks at the previous ten days. This is because the new data has more weight on simple moving averages that consider a narrower period.

The choice of using the 50-day moving average as an example is not causal. However, in our experience, we have seen that it is the one that responds well to price movements while smoothing market excesses. Let us now see how to use this concept to improve the investment strategy of the dollar-cost averaging plan.

The advanced dollar cost average plan

To better understand this strategy, it is best to reverse, i.e., to show its characteristics before analyzing the reasons behind these choices and seeing what data support them. The advanced DCA is structured as follows:

- When the price of Bitcoin is above the 50-day simple moving average, we proceed with a classic accumulation plan with regular investments from month to month;
- When the Bitcoin price closes two candles below the 50-day simple moving average, you sell your accumulated positions;
- As long as Bitcoin's price remains below the 50-day simple moving average, you use the capital gained from the sale to accumulate the downside, with weekly staggered entries;
- As soon as the price of Bitcoin closes two candles above the 50-day simple moving average again, you enter with all your leftover capital, if any.

This might sound not very easy if you've

never invested, but as you'll see, it's straightforward to implement. Let's go through this strategy point by point; when the price of Bitcoin is above the 50-day simple moving average, a monthly DCA is implemented.

This is perhaps the most straightforward case to understand. Each month, the investor will market the amount of dollar corresponding to the percentage dedicated to investing in Bitcoin. Assuming you make trades every 8th of the month, the chart below shows when your purchases would have been made from January 2021 to today.

When the price of Bitcoin closes two candles below the 50-day simple moving average, you sell your accumulated positions.

This step is also not difficult to understand. Closing below the 50-day simple moving average indicates that the uptrend is probably over and that there will be a period of price decline. This would be the best time to capitalize on the gains made during the climb. Expect two daily candles below the average because this gives further confirmation that the hypothesis is probably correct. The following chart shows where positions would be sold from January 2021 onward.

As long as the price of Bitcoin remains below the 50-day simple moving average, it accumulates downward by reinvesting the capital gained from the sale.

Statistically, when Bitcoin falls below the 50-day simple moving average, it stays there for 45 days. This means that the capital from the

sale you just made has to be divided into 45 different parts, which are put to market daily. Suppose the price stays below the simple moving average for more than 45 days. In that case, the amount for the month will be divided to continue to allow daily income.

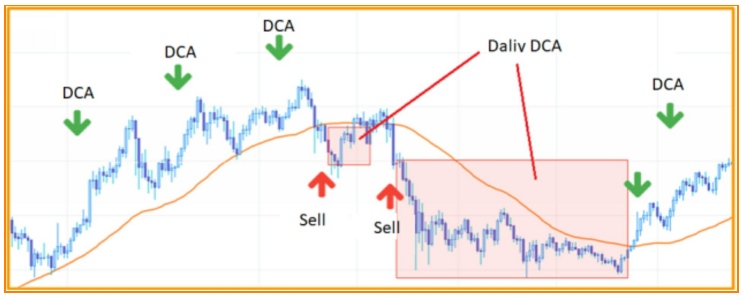
In particular, the chart below shows the areas where the investor would have made daily purchases since January 2021.

As soon as Bitcoin's price closes two candles above the 50-day simple moving average again, you enter with all your advanced capital and resume your DCA.

Suppose the price rises above the simple moving average after less than 45 days. In that case, there is a signal that the downtrend is probably over, and you need to get in with

the remaining capital and resume your accumulation plan. Again, one waits for confirmation given by two daily candles. Visually, this is where you would re-enter with all your capital.

Now let's try to put all the pieces together in one graph:



As you may have guessed, the logic behind this strategy is straightforward: make the most of downturns to accumulate as much as possible for upturns, which statistically occur constantly for BTC, ETH, and ADA. The

strategy of the advanced DCA can also be adopted on these two assets. Later we will talk about the correct division of capital between these three cryptocurrencies. Still, first, it is worth comparing the returns of this system compared to a simple DCA and the investment in a single solution.

To recap

- The advanced DCA tries to beat the performance of a classic dollar-cost averaging plan.
- The basic idea is to profit from positive periods and redistribute them in negative periods to obtain a better income.

Chapter 32 - Results of the Advanced DCA

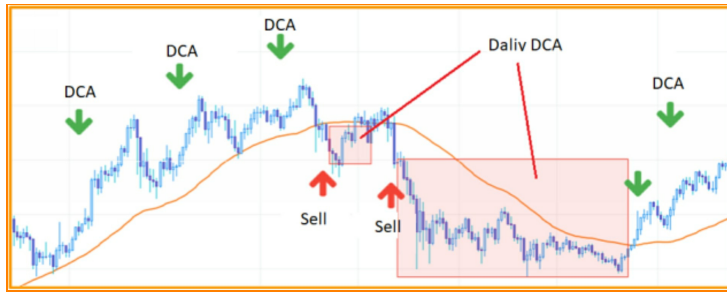
To assess the effectiveness of this investment strategy, it is necessary to compare it with a reference performance. In this case, it is appropriate to compare the results with those obtained with a simple monthly dollar-cost averaging plan.

Let's take the same starting date we used to illustrate the strategy in the previous chapter: 8 February 2021. By investing the same amount every month, we would have bought at these levels:

- 8 February: $46,416
- 8 March: $54,929
- 8 April: $58,096
- 8 May: $57,381
- 8 June: $33,411
- 8 July: $40,352
- 8 August: $46,292

The average entry price would have been $48,125. Therefore, considering the current price, which at the time of writing this book is $49,118, the DCA would have performed 2.06%.

Implementing the advanced DCA, on the other hand, here is what would have happened (for the sake of convenience, we again show the same image as in the previous chapter):



The first three purchases would be equal:

- 8 February: $46,416

- 8 March: $54,929
- 8 April: $58,096

With an average revenue of $53,147.

On April 20, the first sale would take place at $56,503, with a profit of 6.31%.

There would then be an initial period of daily accumulation. Then, finally, there would be an entry with an average price of around $52,000.

On May 12, there would be a second sale, this time at $56,763, with a profit of 11.08%.

This would be followed by a second 76-day accumulation period with daily purchases. In this case, the average entry price would be $41,000. Today, given that the price is around $48,852 and is above the 50-period moving average on the daily chart, we would find ourselves with an unrealized gain of 19%.

As you can see, even in a short period of only eight months, the advanced DCA has given a total return many times higher than the classic dollar-cost averaging plan. As we have seen, Bitcoin is an asset that always

tends to rise over time, and it is advisable to capitalize to the maximum the periods in which it follows a bearish trend.

The advanced DCA would have given better results even of the investment in one solution in the same temporal interval. However, this would only have performed 6.61%.

After seeing these results, we can be convinced that the advanced dollar-cost averaging plan is a strategy that applies to Bitcoin (as well as ETH and ADA since they are relatively related to BTC). It is a way for the investor we have profiled to protect the gains made and make the most of downturns to secure a position ahead of the market.

To recap

- The advanced DCA can perform better than a simple dollar-cost averaging plan.
- In some cases, it even performs better than investing everything at once.

Chapter 33 - Building the Portfolio

We still have to figure out what percentage to allocate capital to the three different cryptocurrencies that reflect the parameters proposed in the book's first part. To approach this question technically, we need to analyze the concept of diversification.

The main objective of diversification is to maximize returns while minimizing financial risk. Typically, this involves determining the person's investment horizon, risk tolerance and sometimes considering broader economic conditions, such as possible regulations or fundamental changes in any asset. Unfortunately, one of the problems for investors trying to diversify for the first time is that they do not understand what they are diversifying into.

Beginners often believe that it is the exposure to an asset that needs to be mitigated. Still, in reality, the financial risk associated with it

needs to be spread across multiple investments.

This is why dividing your capital equally between the top 100 cryptocurrencies by capitalization makes no sense. In this case, you would be diversifying the number of different assets you own. Still, you would not be mitigating your financial risk in any way as, apart from the top 3, no cryptocurrency meets the criteria given above.

To figure out how much percentage to dedicate to BTC, ETH, and ADA, it is necessary to understand the amount of financial risk present in each of these three cryptocurrencies and make sure that it is distributed equally. It would be great if there were a formula or mathematical approach to this issue, but unfortunately, there isn't. Therefore, the only sensible way to resolve this issue is to take up a concept used in the second part of this book: capitalization. Financial risk is directly proportional to capitalization because the less money there is in a system, the easier it is for a small group of participants to control. In other words,

moving the price of an asset with one million capitalizations by one percentage point requires exponentially less effort than causing the same movement in an asset with one billion capitalizations.

Let us, therefore, focus on the capitalization of Bitcoin, Ethereum, and Cardano.

By doing the proportions, we get this information:

- Bitcoin's capitalization is about 2.4 times that of Ethereum and about ten times that of Cardano;
- Ethereum's capitalization is about 4.32

times that of Cardano.

This means that our investor's portfolio will have to consider these values and be weighted on these proportions. Here's how.

We can see that the total capitalization is about 1176 billion dollars (777+324+75). From this value, we calculate how much, as a percentage, each of the three cryptocurrencies contributes:

- Bitcoin → 66%
- Ethereum → 28%.
- Cardano → 6%

So each month, the investor profiled at the beginning of the book will invest 66% of his cryptocurrency capital in Bitcoin, 28% in Ethereum, and 6% in Cardano, and subsequently, withdraw the funds from the exchange to his wallet.

To recap

- To choose how much to invest in each cryptocurrency, you need to calculate how much its capitalization weighs on the total.
- Each month, funds must be allocated according to the calculated percentages.

Chapter 34 – Portfolio Rebalancing

Every six months, it is advisable to rebalance the portfolio to ensure that the proportions always follow any new changes in different capitalizations.

A few practical examples are worth a thousand words.

Case #1

Let's assume that after six months, the capitalization percentages are as follows:

- BTC → 50%
- ETH → 25%.
- ADA → 25%.

In this case, you will need to make the necessary transactions to ensure that your portfolio reflects the current market situation. In particular, here are the operations that the

investor will have to carry out:

- BTC → Sale of 16% to bring its weight in the portfolio from 66% to 50%.
- ETH → Selling 3% to bring the portfolio weight from 28% to 25%.
- ADA → Purchase of 19% increases its weighting in the portfolio from 6% to 25%. The additional purchase of ADA will be made using funds released from Bitcoin.

Also, for the next six months, the investor will invest monthly at these percentages.

Case #2

Let us now assume that Cardano no longer meets the criteria we have repeatedly mentioned (and which can also be found at the end of the book) and should therefore be removed from the portfolio. In this eventuality, the investor will have to do the following:

- Sell all the ADA tokens, bringing their

weight in the portfolio from 25% to 0%.

- Calculate the new percentages of BTC and ETH. Since BTC represented 50% of the portfolio and ETH 25%, this means that the capitalization of Bitcoin is twice that of ETH. Therefore, BTC will occupy 66% and ETH 33% in the new portfolio, so their ratio will remain the same.
- According to the new proportions, distribute the funds obtained from the sale of ADAs into BTC and ETH.

Case #3

Let's assume, lastly, that after another six months, a new cryptocurrency becomes eligible to enter the portfolio. For convenience, we denote this new asset by X. The investor will need to do the following:

- Calculate the new total capitalization of the cryptocurrencies in the portfolio;
- Calculate the relative percentages,

weighing them against the capitalization as done when creating the portfolio;

- Sell and buy the different cryptocurrencies so that the final situation is consistent with the calculated percentages.

Some investors perform rebalancing every month or quarter. However, we recommend at least six months to give the portfolio time to show its results and avoid getting caught up in emotions. As you can see, rebalancing is a highly mathematical and logical process that, if followed to the letter, does not allow for unwise choices and will enable you to keep the financial risk resulting from active management to a minimum.

To recap

- The portfolio must be rebalanced every six months.
- To rebalance the portfolio, the percentages are recalculated, and cryptocurrencies are bought and sold to

achieve the correct proportions.

- Continue with the new proportions for another six months.
- If a project no longer meets the criteria set previously, all positions in that asset are liquidated.

Chapter 35 – Cash Flow Oriented Strategies

Until a few years ago, cryptocurrencies were considered assets beneficial for capital appreciation but not for generating returns. This has changed since around 2019, with the advent of decentralized finance and peer-to-peer lending platforms. So let's look at the possibilities for deriving a recurring income from the portfolio we have built. We will rely on both decentralized solutions and company services.

Cardano staking

Without going too in-depth about the technicalities, as we did in the more academic books on cryptocurrencies, we can define staking as the possibility of validating the blocks of a blockchain by blocking a certain amount of coins. This process is also known as "staking." We can think of staking as

bonds on an investment level: you tie up capital for a certain period, and in return, you receive recurring revenue. At the end of the fixed period, the entire sum is returned to the investor.

Not all cryptocurrencies can be staked. To date, in the portfolio that has been constructed in this book, only Cardano supports this function. Ethereum is moving to fully integrate this consensus mechanism within the next couple of years. Bitcoin, on the other hand, is structurally designed not to allow recurring returns to its holders.

An essential aspect of staking, which makes it entirely secure, is that funds do not have to be sent to third parties.

For the process of staking ADA tokens, Cardano offers two specific online wallets. The first is Daedalus (daedaluswallet.io), a desktop wallet for Windows, macOS, and Linux, created by the development department of Cardano's founding company. The second is Yoroi (yoroi-wallet.com), a wallet that is simply a browser extension running on Google Chrome, Microsoft Edge,

and Firefox. It can also be used on Android and iOS devices.

Because of its ease of use, Yoroi is the recommended choice in this book. Here's how to use it for staking your ADAs:

- To stake ADAs using Yoroi, the first step is obviously to download and install the extension.
- At this point, you need to connect a hardware wallet that contains ADA tokens and transfer them to the Yoroi wallet.
- Lastly, it would help if you chose a "pool" to which you will delegate the staking of your ADAs. A pool is nothing more than a collection of users who join forces to be more likely to be chosen to validate a block and thus receive the associated rewards. Each staking pool charges commissions to its delegators, so it is worth considering the different options available at the time. An investor can also choose to delegate staking to multiple pools simultaneously to reduce financial risk further.

After delegating ADAs to a pool, additional tokens will begin to accumulate. Then, for the first time only, the user will have to wait 20 days to be approved by Cardano's network and see staking results. After this initial 20-day wait, the investor will start earning rewards steadily, which will be credited to the Yoroi wallet every five days.

The return to be expected, to date, is about 4% per year. However, the exciting thing is that this value must be added to the possible capital increase resulting from the appreciation of ADA. Basically, from a financial point of view, staking allows you to mitigate financial risk by making up for a potential price collapse by increasing the number of tokens you own.

For those who don't feel confident enough in their computer skills, some exchanges also include staking ADAs. In this case, the exchange itself acts as the operator of the staking pool and takes care of all the technical aspects. The leading exchange that currently supports staking Cardano is Binance. However, one must never forget that

one increases the financial risk by leaving the funds on a platform outside of one's wallet.

Cryptocurrency lending

The second way to get a return on the portfolio we have built up is to rely on centralized and decentralized finance systems that allow us to lend other users our funds in exchange for interest.

The first solution that we have tested and can also recommend to those approaching investing in this sector for the first time is Blockfi (blockfi.com). It should be noted that this is a centralized solution since the platform is managed by a specific company, Blockfi Lending LLC, which, although serious, is still a company over which the investor has no control.

Using Blockfi is relatively simple: once you have registered, you send the ETH and BTCs you want to put into income to the address on your account, and you start earning interest. Behind the scenes, Blockfi takes care of

lending our coins to investors (who need them for trading) or to large financial institutions that can sell them to their clients. In return, these entities have to repay the loan and interest by a specific date. Blockfi then retains a percentage of this interest and credits the remainder to the user's address on the first day of each month.

As you can see from the image, the returns that can be achieved on BTC and ETH are attractive.

Coin	Amount	APR
BTC	0 - 0.25 BTC	4%
BTC	0.25 - 5 BTC	1.5%
BTC	> 5 BTC	0.25%
ETH	0 - 5 ETH	4%
ETH	5 - 50 ETH	1.5%
ETH	> 50 ETH	0.25%

A similar service is also offered by Nexo (nexo.io), the proprietary platform of Nexo Financial LLC. The operation is identical to Blockfi's; you simply deposit ETH and BTC to your account address and earn interest. On Nexo, however, these are credited daily, and the return percentages are slightly more

favorable.

Coin	APR
BTC	8%
ETH	8%

The Crypto.com exchange (crypto.com) also allows users to receive interest from lending their cryptocurrencies; in this case, returns are credited every seven days, and returns are slightly higher than those obtained using the other two proposed solutions.

Coin	APR
BTC	8.5%
ETH	8.5%

To mitigate the financial risk associated with outsourcing the holding of your cryptocurrencies as much as possible, our advice is to distribute the return portion of your capital equally among these three solutions.

But what percentage of the portfolio should be put into income? The answer is twofold.

For ADAs, given that you never lose possession of the tokens, it is advisable to stake the entire quantity.

For BTC and ETH, since the solutions that allow returns are centralized, the advice is to dedicate a maximum of 30% to generate an income, dividing the funds equally between Blockfi, Nexo, and Crypto.com. This way, you can get about 6.83% on 30% of your portfolio, which on the total invested means adding an extra 2.27% each year. This is an outstanding return, and further reduces the financial risk associated with possible capital depreciation.

To recap

- Two methods are used to earn income from the portfolio you create staking and borrowing.
- Staking can only be done on ADA through the Yoroi wallet.
- To lend your BTC and ETH in exchange for interest, Blockfi, Nexo, and

Crypto.com are used.

Chapter 36 – Portfolio Overview

In this course, an attempt has been made to bring a rational approach to investing in cryptocurrencies. This is no easy task, given the enthusiasm that quickly builds up around this sector in bullish phases and the desperation that dominates the hearts of investors during downturns. After analyzing data and statistics, here is the recommended portfolio for the investor profiled at the beginning of the book.

Asset Allocation:

- BTC → 66%.
- ETH → 28%.
- ADA → 6%.

Investment strategy:

- The advanced dollar-cost averaging plan
- Rebalancing every six months
- 100% of ADAs are brought to income by

staking on Yoroi

- 30% of BTC and ETH is equally allocated and earned through loans on Blockfi, Nexo, and Crypto.com.
- The remaining 70% of BTC and ETH remains safe on a hardware wallet.

To be able to keep track of portfolio performance, the recommended tool is CryptoCompare (cryptocompare.com). It is very simple to use: enter the number of coins held and the entry price to obtain a performance graph. The graphic is exceptionally user-friendly and allows to have all the information that can interest the investor at a glance.

The image below is CryptoCompare's presentation of one of our wallets. If you have studied other books on this topic, you know that it is not common to show concrete results. This is because fewer people invest in cryptocurrencies than you might think. We wanted to distinguish ourselves in this respect as well. There are already enough charlatans,

and money doesn't like to talk.

As trivial as it may sound, we would like to stress that when you enter data on CryptoCompare, you are not mobilizing funds from your wallet. Instead, this platform is merely a way for you to keep track of your returns and have all the information you need at your fingertips for your semi-annual rebalancing.

Chapter 37 - Monthly Process for Using This Portfolio

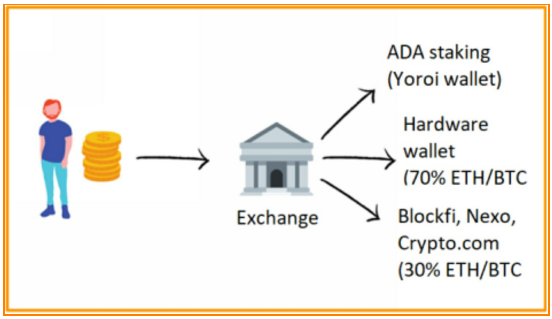
Let us conclude our journey by summarising the steps the investor must take each month to build and carry out the portfolio according to the strategies examined above.

- At the beginning of the month, the investor calculates how much 20% of the capital dedicated to investments corresponds to and deposits it on the exchange of his choice.
- Once the funds have arrived on the exchange, he buys BTC, ETH, and ADAs in the indicated proportions and according to the Advanced dollar-cost averaging plan.
- Next, the ADAs are sent to the Yoroi wallet, staked to generate an annuity.
- 70% of BTC and ETH are sent to a hardware wallet to eliminate the financial

risk of holding on exchanges.

- To earn an income, the remaining 30% of BTC and ETH is split and distributed equally across Blockfi, Nexo, and Crypto.com.
- Every six months, the portfolio is rebalanced to reflect the new proportions dictated by the capitalization of the individual projects.

The following infographic shows this process.



It is likely that, after an initial period of getting to grips with the technicalities, this is a process that takes about twenty minutes a month at most. The invitation is not to get caught up in the urge to trade all the time,

buying and selling beyond what the strategy you want to follow suggests. This is good to point out because, from experience, we know that it is inevitable to want to "do" to feel more in control. In reality, investing in cryptocurrencies should be as passive as possible, like investing in other assets. You work all day to generate money, and it's only fair that investing it should be working for you.

PART 9 – CRYPTOCURRENC TRADING

Chapter 38 – What is Online Trading?

Online trading is the buying and selling of financial assets over the internet. Buying and selling are done through software that is usually called the trading platform. Trading platforms are created and made available to customers by financial companies called online brokers. Brokers buy and sell assets on behalf of their clients and charge a commission for the trades they perform. Brokers can be banks or companies specializing in online trading. And for non-professional investors, you can also rely on cryptocurrency exchanges.

Online trading is an inexpensive way to invest your money in the cryptocurrency market. Commissions are low, and you have access to real-time quotes and charts, technical and fundamental analysis of crypto assets, and many other things. With online trading, you have to monitor data in real-time.

Online trading is suitable for those who want to invest their money alone. But to take advantage of the independence that online trading makes possible, you have to work hard. This means that you have to study, apply a strategy and resist market pressure. Cryptocurrency markets are, in fact, very complex and, above all, unpredictable. This is why we need to study a lot and, above all, continue to define and adapt our operations to possible changes in the scenario.

The volatility of the markets also puts a strain on the trader's character. It is not easy to maintain an operational strategy when the market goes against you. For this reason, you need the exemplary character to avoid being overwhelmed by emotions.

To go into greater detail on how to trade online, let's now focus on the use by the investor and identify three ways of operating (based on the time horizon that the investor decides).

Scalping is the entry and exit from the market, usually with stocks, several times

throughout the day (operations that last minutes).

Day trading, which means operating with a daily time horizon. The day trader buys a stock, which he has been following for a certain period, and believes it that day because he is convinced by his analysis of him, from the news of the stock and the market, that he will perform the best that day.

Then there are the open traders, or those who enter the market randomly or after some data or news release.

There are also long investors. And that is, those who open long positions believe that stock, given certain events, can rise over a medium-long period.

Chapter 39 – Fundamental Analysis

Fundamental analysis is a tool used by traders to evaluate and study the variables that affect the value of an asset. This tool focuses on studying the factors, events, or external influences that affect the price of an investment. The first mentions of fundamental analysis began in 1934. At that time, Benjamin Graham and David Dodd introduced this concept in their book Security Analysis.

Since its inception, fundamental analysis has been a handy tool for analyzing markets. This is because Fundamental analysis focuses on how external factors affect a stock's value, unlike technical analysis, which focuses on studying the charts of a market to predict how the asset will act.

In fundamental analysis, the most common analysis tools are:

- The periodic balance.
- Analysis of financial reports

- Asset or company valuation techniques.
- Economic forecasts: analysis of the environment.
- General economic information.
- Any additional information that affects the value of a security.

Different approaches to fundamental analysis

In fundamental analysis, two types of approaches seek to offer the best response to the investor. These approaches are thought to analyze micro and macroeconomic variables in one way or another. So we are left with the following types of methods.

Top-down

In this type of fundamental analysis, the macroeconomic variables are studied before the microeconomic variables. This means that decisions are made with global information first until the most detailed and specific values and variables are considered. An example of this approach could be a multi-level analysis as follows:

- Study of the world economic situation
- Study of the most attractive countries to invest
- Within each of these countries, the sectors with the most significant potential are chosen.
- Within the sectors with the most significant potential, the most interesting ones to invest in are analyzed.

Bottom-up

This approach focuses first on the microeconomic variables and then on the macroeconomic variables. In this case, contrary to the Top-Down approach, we start from a more specific view up to a more global perspective. For instance:

- Companies that have growth potential are chosen.
- An analysis of the sector or sectors in which these companies operate is then carried out.
- The economic situation of the country or countries in which they operate is studied.

- Finally, the global economic situation is analyzed.

Advantages and disadvantages of fundamental analysis

Like any tool, fundamental analysis has advantages and disadvantages in its use. Below we will explore some of them to get to know them.

Benefits

Among the advantages of fundamental analysis we can mention:

- It allows investors to collect and analyze information external to the internal reality of the markets. This allows the investor to have a clearer view of the market reality. The new data will let you know how the values react to different events.
- It offers a complete understanding of the value of an asset. This way, investors can more accurately extrapolate the future value of that asset. This offers certainty when investing.
- It allows for greater freedom of action

than technical analysis. This is because fundamental analysis leads us to make medium and long-term decisions. By comparison, the technical analysis shows us to act more repeatedly on the markets to adjust our choices to the information provided by this type of analysis.

Disadvantages

However, like any tool, the fundamental analysis also has drawbacks, and some of these are:

- The need for extensive knowledge and experience to perform a good analysis. Sound fundamental analysis requires knowledge of accounting, business, and more specifically of the sector in question in which the asset of our interest is located. This knowledge must also be accompanied by experience. This will finally be the one that will allow you to make better decisions based on the information analyzed. Simply put, applying a fundamental analysis is more complex than a technical analysis.

- The investment terms with fundamental analysis are longer. This is because a fundamental analysis takes more time and study than a technical analysis. This leads the investor to wait for certain market levels to know whether to buy or sell.
- Although fundamental analysis offers a much broader view of the markets, it can be overwhelmed by random factors. A flood or drought affects the price of cereals, or a war affects the price of oil and other commodities. Probability factors are one of the most severe problems in fundamental analysis because they cannot be fully predicted. To this, we can add negative legislative, political, and economic changes that surprise the markets.

In the case of crypto markets, the fundamental analysis can analyze the external reality that affects them. This is extremely important, as the cryptocurrency market tends to react quickly to external factors due to its

unpredictable situation in the world. For example, regulatory pressures from countries like the United States, the European Union, or China significantly impact the price of cryptocurrencies. Quite an understandable question and that this same tool can help us understand.

Faced with these events, fundamental analysis becomes more critical to recognize the fair value of crypto assets. Crypto market investors tend to use technology to make them happen quickly. It is not uncommon, for example, to see market data and external factors available in Slack, Telegram, or Reddit. During an increasingly interconnected world, the use of technology to perform these analyzes takes on greater value.

Furthermore, among the main factors observed by the fundamental analysis in cryptocurrencies, we can mention:

- Usability and adoption. This point is intended to examine the usability and adoption of a cryptocurrency—the simpler the use and the greater the adoption of

cryptocurrency, the greater its actual value.

- Position of governments and regulations. This point is intended to study how governments view a specific cryptocurrency and whether or not it complies with regulations. A favorable regulatory framework will increase the potential of the cryptocurrency, or if it is unfavorable, it will limit its potential.
- Project development and media coverage. Investigate how the development of the cryptocurrency project is progressing. The development activity of the cryptocurrency, its software, its community, and increased media coverage will indicate that the cryptocurrency has the potential for greater value.

Chapter 40 – Technical Analysis

Technical analysis is a branch of the study used to predict the future direction of prices by studying historical market data. This technique uses data relating to prices, volumes, and open interest in a market to achieve this.

This means that technical analysts use trading data along with mathematical indicators to make their trading decisions. The result of these formulas is automatically reflected in a graph updated in real-time, which will interpret the trader's file to determine when to buy or sell.

Thanks to the technical analysis, it is possible to predict the direction of the prices, which has made it one of the main tools for forecasting the behavior of the financial markets. This latter aspect is especially true when combining technical analysis with fundamental analysis. The combination of both types of analysis allows traders to have a

complete assessment of the reality of the market. Thanks to this, traders can get a clear advantage when making profitable trades.

In market research, the two most used analysis tools are technical analysis and fundamental analysis. Technical analysis originated in the United States in the late 19th century. Its creator and leading exponent were Charles Henry Dow, creator of Dow Theory. The purpose of technical analysis is to identify trends or patterns and allow traders to make action decisions within a market. To achieve this, the technical analysis uses several graphical and mathematical tools to predict these trends and decide.

Furthermore, fundamental analysis is a tool first developed by Benjamin Graham and David Dodd in 1934. The idea of fundamental analysis is to calculate the value of an asset using the balance sheet data of those assets and compare them with what is observed in the market. With this, it seeks to provide the best view of the action to the trader and allow him to take a stand against that action.

The purpose of both tools is the same: to offer a market analysis tool to traders to make the best possible decisions at all times. Something that both tools undoubtedly do successfully.

Principles of technical analysis

Technical analysis has several pillars that support its validity. When Charles Dow developed his theory of himself, he summarized these principles as follows:

The price discounts everything. This is an essential principle of technical analysis. This principle indicates it; all information is included in the price. That is political factors, wars, reports on the profits of a company, social situation of a country. Therefore, everything is discounted in the quote. This means that all that local or global action that can impact a specific value will be reflected in its price.

Markets are trending. This is a situation that occurs all the time and without exception. Trends can be up, down, or sideways. Charles Dow explained that an asset is trending until

you prove otherwise. This means that; until the maximum or minimum reference is exceeded, the trend of that value continues.

Human behavior is repetitive. Human psychology is predictable because its mass behavior is cyclical and responds similarly to similar events throughout history. Under this precept, the technical analysis states that; Pricing models are subconsciously created that reflect this behavior. Thanks to this, the study of him allows you to predict future price movements, as they are influenced by the psychology of the group related to it.

Origin of technical analysis

Technical analysis originated in the United States at the end of the 19th century. Its creator and leading exponent were Charles Henry Dow, creator of the Dow theory. This theory gained significant momentum with Ralph Nelson Elliott within the stock markets with his Elliott Wave Theory. It was later extended to the futures market. However, its principles and tools apply to the study of the charts of any financial instrument.

Technical analysis can be divided into two categories:

- Graphical analysis or graph analysis: Without additional tools, only the information revealed in the graphs by predominantly geometric figures.
- Technical analysis in the strict sense: uses indicators calculated based on the various characteristic variables of the behavior of the analyzed values.

Technical analysis tools

Candlestick chart

This type of chart is most used to visualize and analyze price movements over time for stocks, derivatives, currencies, stocks, bonds, commodities, etc. They are also known as the Japanese Candlestick Chart, as they originated in that country. Candlestick charts display various price information such as opening price, closing price, highest price, and lowest price through candle-like symbols. These represent a compressed trading activity for a single period (one minute, hour, day,

month, etc.). Each candle symbol is defined along a time scale on the x-axis to show trading activity over time, while the y-axis represents the price. They are handy for their versatility and their usefulness in detecting and predicting market trends over time.

Charts

Charts are graphical representations used to organize the information contained within a market. In general, financial and cryptocurrency markets use bar charts or line charts to represent the real-time flow within a market. The reason behind using these graphical tools is to synthesize the most significant amount of information in a single box, allowing for a better understanding of that information. Charts are often used to facilitate the understanding large amounts of data and the relationships between parts of the data.

This is very useful in a financial market where information on stock values changes rapidly, and data flow is constant.

Indicators

Technical indicators are statistical-based tools for determining future market behavior. These are the four general categories of indicators:

Trend: These indicators are used to detect trends in the financial markets. This group of indicators is inefficient for market flat periods. Trend indicators indicate the direction of price movement.

Impulse: This is an oscillator-type indicator that shows the price trend and the changes it has had over a specific time. Its function is to anticipate trend changes and teach the speed of price change. The exercise consists of observing the price difference between the end of the current period and that of the previous days.

Volatility - These indicators analyze the changes in market prices over a given period. The faster the prices change, the greater the volatility and, conversely, the slower, the lower the volatility. It can be measured and calculated based on historical prices as well as to identify trends. It usually indicates whether a market is overbought or oversold

(meaning the price is unjustifiably high or low) and can indicate stagnation or a turnaround.

Volume: they are used to study the volume of a market, allowing you to relate the evolution of the volume with the price changes.

Benefits

One of the main benefits of this tool is identifying price trend signals in the market. This is a critical factor in any trading strategy while trading. Thanks to this, investors can develop a successful methodology to locate entry and exit points in the market.

Another advantage is that technical analysis tools are widespread and easy to use. They are so common that some believe they have created operating rules that conform to themselves: the more investors use the same indicators to find support and resistance levels, the more buyers and sellers will be interested in the same ranges. As a result, prices and patterns will inevitably repeat themselves.

Disadvantages

One major drawback of this tool is that there will always be an element of market behavior that is unpredictable. This situation is closely related to Random Path Theory, presented by Louis Bachelier in 1900. This theory indicates that:

"Any change or evolution in the financial markets is not measurable and estimable due to their randomness and efficiency. He also stresses that it is impossible to make reliable predictions of the price of assets just by studying their past evolution".

That is why there is no guarantee that one type of analysis is 100% correct. While historical pricing models can give us an idea of an asset's possible price trajectory, this is not a guarantee that it will happen.

Investors should use various indicators and technical analysis tools to achieve the highest level of security possible and have a risk management strategy to protect themselves in difficult times.

Chapter 41 – Basic Technical Analysis Indicators

After choosing the cryptocurrencies to trade, reading the charts that show the price trend is essential. The market trend is the trend of prices that a particular market is following. The movement is used both for backward analysis and for making predictions.

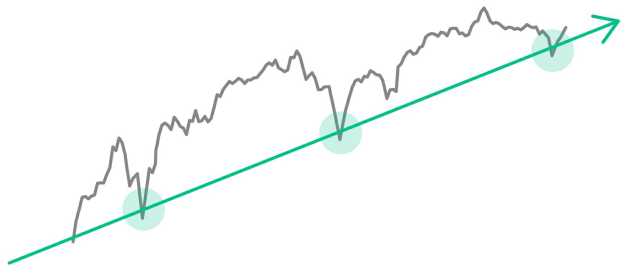
Trends can be in several stages:

- Bullish: when a market trend is in a bullish phase. We will see a clear rise in prices on the graph.
- Bearish: when the market trend is in a bearish phase. We will see on the chart a clear reduction in prices.
- Side phase: when the trend is in a stalemate and prices remain stable, without precise direction.

Linear charts can be easily found for each type of cryptocurrency and show the

historical trend of prices. By observing these charts, trendlines can be created. Within a chart representing the trend of any cryptocurrency or financial asset, a trendline is a straight line drawn to help you read and analyze this trend. Now let's see how to draw the trendlines and configure them when they are bullish or bearish.

Let's take a chart representing the price trend over a certain period and start drawing the line from the first evident price peak, whether positive or negative.



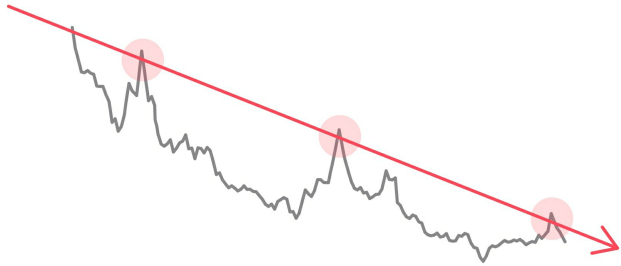
Let's start with a negative peak. Then, if an upward trend can be traced after a short drop in the price, increasing-price lows are

identified, as in the image. So let's combine all the price lows with a line that will go up.

The trend indicated by this line is called bullish. It is like a bull that charges all the obstacles in the market with its aggressiveness.

A bullish trend market is called a bull market.

When no higher lows are encountered, it means that the trendline has reached a breaking point and is likely to turn bearish.



Let's move to the high side of the trend represented by the chart and focus on the positive price peaks. If there are no more increasing lows, we must go and look for

decreasing maximums. Once we have identified some falling price peaks on the chart, let's join them with a line that will point downwards.

The trend marked by this descending line is called bearish, like a bear that wants to hibernate. A bearish trend market is called a bear market.

Now that we are familiar with the cryptocurrency markets tools let's take it one step further. Let's try to understand how real experts read charts. You have indeed seen these strange charts made up of red and green vertical candles. The poetic name knows these candles of "Japanese Candles."

The story behind this type of chart is as exotic as its name. The invention of these dates back to the seventeenth century in Japan, intending to predict the rice price trend.

Now let's see how candlestick charts are read: in this way, we will understand why they are so helpful.

The candles summarize the price movements

over a predetermined time interval that can be selected from the interface. This time can be a minute, a day, a month, or a year.

Let's take as an example a candle that symbolizes the trend in the price of bitcoin in a single day.

The chart in full will therefore represent the trend over a certain number of days.

Let's assume that during Day 1, represented by a single candle, these changes in the price of bitcoin occurred:

Day 1 for BTC

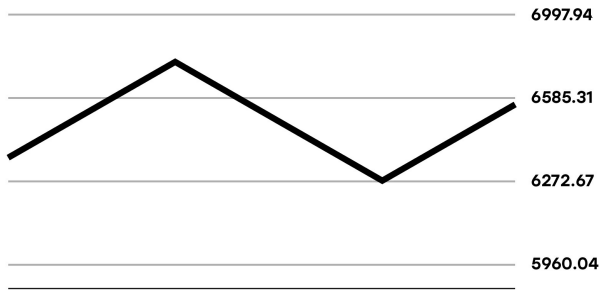
Opening: $ 6330

Maximum: $ 6,620

Minimum: $ 6272

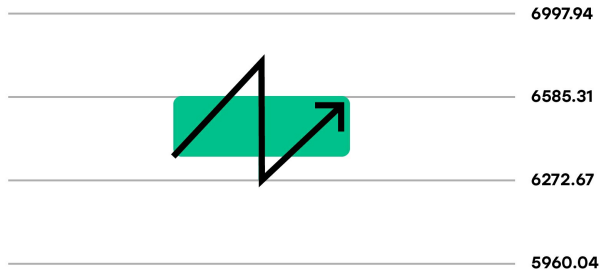
Closing: $ 6585

The movement that we will see on a classic linear graph will therefore be:



This is a positive trend, as the final price is higher than the one at the beginning of the day.

The candle representing this movement will be green and will look like this:



The candle's body, i.e., the central part in

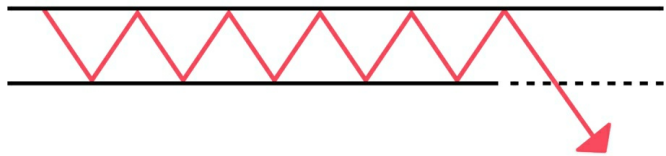
green, represents the difference in price between the beginning and the end of the day. The lower end, which marks the price at the beginning of the day, is called "opening" (open) because it marks how the day started. The upper end, which marks the price at the close of the day, i.e., the last recorded, is called "closing" (close).

The lines above and below the body are called wicks. They represent the maximum and minimum price reached during the time interval. Shadows are, however, essential in advanced technical analysis and should not be underestimated.

Candles are much more detailed representations of the price trend than a classic linear chart. Therefore they lend themselves to advanced technical analysis. If we consider that the Japanese have been using them for 300 years and have taken the trouble to name every possible candle configuration - as if they were tai chi positions - there is a reason.

Supports and resistances

The support and resistance lines are fundamental parameters for understanding the behavior of a cryptocurrency and making assumptions. Just like trendlines, they are lines that can be found on a price chart. Candlestick charts are always preferred for these advanced analyzes. However, to explain the concept of support and resistance, we use a more linear representation. So let's imagine a game like pinball, in which there is a ball that zigzags between two walls.



The bottom wall will be the support, and the

top wall will be the resistance. These two walls represent the "upper and lower" extremes that the cryptocurrency in question continues to reach and fails to overcome. Failure to break through these levels (both up and down) in a given period is a symptom of the market not having the strength to take a direction.

For example, suppose during a given period, bitcoin fluctuates, reaching $10,000 several times, but fails to go higher ("breaking through" that particular price). In that case, that is the resistance of $10,000.

There is no mathematical method to identify these lines because different schools of thought employ various ways to trace them. Therefore, it is up to the trader to identify the pattern in the trend that he is observing and interpret it.

The only secret to identifying and drawing these lines is to practice a lot. Only through practice and by observing the experts who draw their lines and following the analysts who use them will you see the lines in formation and even anticipate some price

movements.

A complementary tool to chart analysis is calculating the moving average (more on that in the next chapter), which helps estimate the average price over a given period.

The theory says that supports and resistances can be identified over any period. However, it is not sure that this type of pattern is identifiable in all cases. Their absence could also be an element to be taken into consideration. Usually, the longer a line is displayed, the stronger it will be in terms of capitalization and impact.

Chapter 42 - Moving Averages and MACD

The most used group of technical indicators is undoubtedly that of moving averages. They are a series of useful mathematical tools that allow above all to smooth out erratic price fluctuations.

A moving average is an average of a certain amount of data that considers only the latest measurements in order of time. This instrument is defined as "moving" because the number of elements considered (the prices) is fixed, but the time interval varies. Therefore, the old data must be removed when new ones are added: this causes the average to move in progression with the trend in the price of the cryptocurrency being calculated. A 200-day moving average, for example, examines the values of the last 200 sessions and is recalculated every day, adding the latest data and excluding the most remote from the calculation so that only 200 prices are always considered.

Usually, the closing prices of the day are

considered. Still, the maximums, the minimums, or the opening values of trades can also be used. This is true if you study a chart with daily data, but we can use hourly, weekly, monthly or yearly closures.

There are various types of moving averages: simple, exponential, and weighted. Each of these has a different calculation method.

The Simple Moving Average, also called arithmetic moving average, is the most used because of its more accessible construction. First, the data of a given period are taken. Then, the average is calculated by adding them together and dividing them by the total number of values. Unfortunately, the greater simplicity of calculation is paid for with a significant defect: this algorithm assigns the same importance to every input; the last value (perhaps even very distant in time) has the same significance as the first.

The Weighted Moving Average tries to solve this problem by attributing greater importance to the most recent data and less to those more distant in time. Taking, for example, a 10-period average, the closing of the tenth and last day is multiplied by 10, that

of the previous day (ninth) by nine, that of the eighth day by eight, and so on. The total will then be divided by the sum of the multiples: in our case 1 + 2 + 3 + ... + 10 = 55. The average is therefore much more reactive to recent events while "dampening" past fluctuations.

A simple 10-day moving average weighs the most recent price precisely like the most distant one, for 10% of the total; the weighted average, on the other hand, assigns a weighting of 18% to the last number, while to the more distant one by 1.8%.

The exponential moving average calculation system is even more complex, an indicator that is almost impossible to generate except through appropriate calculation software. All available data are considered - not only those relating to the period under consideration - even if the domain prices, particularly the most recent ones, have a greater weight. This average is constructed considering all the elements of the series but with an exponentially decreasing importance. The weighting of the first data of the series will be smaller over time until it becomes

infinitesimal. Still, it will always be included in the calculation. The entire history of the title is taken into account.
Since their function is precisely to follow the current price movement, moving averages are the indicator par excellence in the so-called "trend following" type "trading systems"; another excellent factor relating to these indicators is the ease of construction and the partial elimination of the subjectivity factor.
However, their signals cannot be generated except with a decent delay.
The simplest method of use is to consider them on a par with trendlines, consider them as natural resistances / dynamic supports, and make decisions when prices break them.
This type of function tends to dampen erratic prices. The effect is more evident the greater the number of events included in the moving average calculation. A moving average, in fact, graphically is a curve that follows the price line, positioning itself below it in the case of an uptrend or above it in the case of a downtrend. The moment the average "cuts" prices usually indicates the moment of change in the trend for the time horizon

defined by the domain. More precisely, there will be a buy signal when prices rise above the moving average, while it will be time to sell when they fall below. It should be borne in mind that the period used has a considerable influence on the indications generated: if you choose a smaller domain, you will get a moving average much closer to the prices which will result in more excellent timeliness, but a more significant number of false signals; on the contrary, a more extended period will give rise to a smoother line that will provide more reliable suggestions, but later than the other.

The problem is partially overcome by using a combination of two averages, one slow and one fast. This system is the most used by analysts. The operational signals are provided at the intersection between the two averages: when the faster one, or generated by a shorter period, crosses the slower one upwards, a suggestion to buy will be generated; vice versa, when the slow one will be cut down by the faster one, the sale will take place.

The use of two averages is the basis of the MACD (Moving Average Convergence /

Divergence), an oscillator with complex construction, but which has the advantage of limiting the analyst's subjectivity in his study.
It is calculated by subtracting the value of a 26-period exponential moving average from a 12-period moving average. This data processing gives rise to an oscillator that combines it with its own 9-period exponential moving average. Buy signals are generated when the MACD lowers its moving average; conversely, sell signals are generated when the MACD breaks its moving average down. Thus, the MACD can make exciting suggestions, especially during a definite trend market; sometimes, it creates false signals in markets that move sideways.
However, the size of the domain always remains the main problem in using moving averages: there is no universally valid value, just as there is no construction method (arithmetic, weighted or exponential) that is always superior to the others.
John J. Murphy, in "Technical Analysis of the Financial Markets: A Comprehensive Guide to Trading Methods and Applications," John J. Murphy, based on data collected by Merrill

Lynch over seven years, undertook an accurate study of the behavior of various types of moving averages across 13 commodities markets. The period considered price movements from 3 to 70 days. Three exciting conclusions derive from this powerful study:

- The simple moving average turned out to be the best, outperforming the performances generated by the weighted and exponential averages. On 13 markets tested, the simple moving average worked well in 10 cases, the weighted one in 2 cases, while the exponential was valid only in the cocoa market;
- The long-term moving averages generated higher profitable trading signals than the short-term ones.

However, no moving average was the best for each market. Instead, each commodity proved to have its optimal moving average.

Despite the undoubted usefulness of these algorithms in investment decisions, it is never possible to completely get rid of subjectivity: the choice of the reference period and the

type of media to be used, as well as the interpretation of the results, are always left to the analyst's sensitivity.

Chapter 43 - Linear and Logarithmic Charts

To analyze a cryptocurrency, the technical analyst must necessarily have a complete historical series of data on the asset he intends to study. The necessary data are those of the prices and - possibly - of the volumes traded, obtainable by detecting daily the prices of a specific security, thus graphically plotting the time variable on the x-axis and the price variable on the y-axis. At this point, the critical problem arises of the scale with which to represent prices. While for time, a linear quantity, one can only use a linear arithmetic scale. This is not so automatic for prices. Remember that prices and time are not homogeneous values, so it is necessary to use the same scale: in theory, BTC, ETH, and ADA would not be directly comparable with a minute, an hour, or a day.

For example, we could prefer a graphic representation that considers not the absolute price recorded on a given day but the

variation recorded by the prices on the given day compared to the previous one. In other words, to represent prices, we can choose a linear or a logarithmic scale. The two modes of representation can make the following two graphs appear decidedly different. In reality, they both refer to the same share in the same period.

The linear (or arithmetic) scale is, of the two, the one used most frequently, also because the logic on which it is based is straightforward. The exact distance is attributed to equal "absolute" price changes. Thus, in practice, if the security price goes from 10 to 20 dollars or 1000 to 1010 dollars, the amplitude of the two increases - always equal to 10 dollars - will be represented identically.

The logarithmic scale is instead derived by calculating the logarithm of the returns. The price variation between the various time intervals is represented on the axis (hours, days, weeks, etc.). This implies a very different representation of the space between

10 and 20 and that between 1000 and 1010 of the above example: think that the first case reflects a variation of 100%, while the second reflects a modest appreciation of 1%.

The best type of chart

In reality, there is no single and absolute answer. The main advantage of using a logarithmic scale is undoubtedly that of identifying, with a simple glance, the importance of movements beyond the fundamental values at which they occurred. Analyzing any financial asset with substantial fluctuations over time is less complicated using this representation, which is also the best for very long-term analysis.

On the other hand, the linear scale allows us to grasp the figures that the market draws along its path with relative ease. Therefore, it is more beneficial for traditional graphic analysis. Often, integer values of prices (10, 50, 100, 10,000 ...) represent critical "psychological" thresholds, testifying that it

is precisely the prices expressed in absolute values that attract attention and not the logarithms of their variations.

Chapter 44 - Dow's Principles

The founder of the Wall Street Journal and inventor of the Dow Jones Industrial Average index, Charles Dow is universally considered the father of technical analysis. In fact, at the beginning of the 1900s, he laid the theoretical foundations by affirming the basic principles of the discipline.

Dow aimed to be able to use the behavior of the stock market as an index of the general trend of the economy. The continuous observation of tidal movements inspired dow. He derived some general rules: waves increasing in size and power signal the arrival of high tide. In contrast, the low tide is anticipated by a progressive weakening of the strength of the waves.

This also happens on the graphical representation of the price trend of a stock or an index. When the successive fluctuations touch more significant peaks ever, a phase of

"high tide," or an increasing trend, can be identified, vice versa. When the subsequent fluctuations affect ever-lower values, we can speak of "low tide," of a downward trend.

Charles Dow developed two market indexes in 1897, the Industrial Average and the Rail Average. These are indexes that are still used today and which have taken the name of Dow Jones Industrials Average and by Dow Jones Transportation Average.

The principles identified, however, can also be applied to cryptocurrencies.

After the historical introduction, it is necessary to deepen the basic principles on which the theory and, therefore, the practice of the technical analyst is built. Principles that emerge from a strictly empirical analysis but are easily found in the daily trend of the financial markets:

Prices discount any available information. The technical analyst believes that the market level of any cryptocurrency is the result of the combination of all the political, economic and

financial news and expectations that can theoretically modify its performance; consequently, in the "technical" study of the price, all the available elements useful for a forecast processing are already included;

Prices move according to a trend. This point is the central point of all studies involving a chart. Without accepting this statement, the study of graphs loses its meaning. It is not so evident that this postulate is recognized as valid. According to some traditional economic theories, such as the "random walk," it is impossible to claim to identify a definite trend for the financial markets. To the skeptics, the technical analyst can only oppose empirical experience;

History repeats itself. These principles are based on the study of human psychology: since the behavior of the markets is dictated by human decisions and since human attitudes tend to remain similar in similar situations, it follows that even the graphical trend of the markets will tend to be identical to that passed on the occurrence of similar

situations. From this assumption derives the part of the technical analysis best known to non-experts, the one that deals with the study of chart configurations (double highs and lows, bullish and bearish head and shoulders, to name a few) whose reliability derives precisely from the fact which reappears with similar characteristics in subsequent market phases.

How to spot a trend

As we have seen in a previous chapter, a trend is identified by a series of highs and lows, which are successively increasing in the case of an upward trend, decreasing in the case of a downward trend, and remaining so until the opposite condition occurs. Therefore, it is up to the technical analyst to identify the directional phase of the market and recognize the potential critical levels of reversal or continuation. Suppose it is impossible to identify a dominant direction in the price trend. In that case, it is more correct to speak of a lateral movement rather than an absence of a trend.

The primary function of technical analysis is the recognition of these three types of trends and the transition from one to another. It is, in fact, mainly around the reversal phases that the operational strategies will be structured. However, if it is relatively easy to recognize the type of trend with which prices are moving in some cases, it is necessary to resort to more sophisticated tools than simple observation to determine the direction of the movement. The search for the answer to the question "what kind of trend am I in?" - which should be the basis of the study of each chart - sometimes it is not immediate: precisely to try to find an answer in every situation, even the less intuitive ones, that all the different lines of study of graphs that go by the name of technical analysis.

PART 10 - CONTROL YOUR EMOTIONS

Chapter 45 - Keeping Your Emotions Under Control

Controlling emotions while trading cryptocurrency is essential, as it can make the difference between success and failure. State of mind has a significant impact on your decisions, mainly new to cryptocurrency trading. Keeping a calm attitude is essential to achieving results.

In this chapter, we explore the importance of controlling emotions when trading for both novice and experienced traders. Although we all know that emotional experiences lead to a wide range of behavioral and cognitive changes, the psychology of trading is often overlooked in education.

From 'revenge' trading to impulsive operations, however, it is clear that a trader's personality is as essential as his knowledge and expertise. To become a professional in the trading field, it is necessary to be flexible, self-disciplined, informed, and ambitious at

the same time, all signs of high emotional intelligence.

Emotions in cryptocurrency trading

Should you listen to your heart or your head? This is the real question. The truth is that emotional responses have been naturally of evolutionary importance, so it's no surprise that traders aren't immune to them.

Only when we learn to recognize and manage our mental responses can emotions help us become winners in cryptocurrency trading.

Negative coping strategies

It is no secret that the roots of our decision-making strategies lie in our childhood. Conditioned to react in a certain way, people transfer their childhood experiences into their adult life. Unfortunately, traders are no exception, and some start trading without being aware of their coping strategies. A coping strategy is a process of adapting to

stressful situations.

For example, a person who was never praised as a child may internalize shame and view their business losses as a personal failure. The truth, however, is that trading is like a minefield full of unexpected results, and the only sure thing is its uncertainty.

Fear and cryptocurrency trading are not a good match

Taking risks and learning to let go are two essential steps to becoming a good cryptocurrency trader. While we must agree that losing a trade can trigger unpleasant emotions and fears, fearful actions are not advisable.

Interestingly, in the popular trading book "Trading in the Zone," known as the bible of trading psychology, Mark Douglas describes three common fears: fear of losing, fear of making a mistake, and fear of letting a victory turn into a loss.

While fear benefits survival in nature, both

fearful economic behavior and loss aversion can play a trick on you. To give an example, even when you have a good chance of winning a trade, your fear can cloud your decision-making strategies and make you exit the operation too early or too late. Unfortunately, numbers show that over 80% of retail traders lose money.

The antidote to fear is confidence. While confidence is essential for success, excessive trading confidence can play a trick on your strategies. Greedy traders often risk large sums in trade, leading to huge losses and negative feelings.

Here we should note that trailing stops can be a valuable strategy to help trading enthusiasts control their greed and reduce losses. Additionally, traders are encouraged to keep position sizing consistent when trading.

Cognitive bias and euphoria

Greed can lead to unrealistic feelings of superiority and euphoria. Attracted by excessive security, some traders tend to place

unplanned trades and forget their trading strategies. Recency bias is a common psychological flaw among traders. Recency bias is the mental tendency to focus solely on the most recent trading periods and winnings.

Another common mistake triggered by biased decision-making is confirmation bias, defined as the tendency of people to look at data that can support their ideas. To give an example, an overconfident trader can ignore information and charts that compare their unrealistic ideas.

However, it's not just the euphoria that can cloud your trading decisions. Any strong emotion or deep feeling can have the same negative effect. One of the worst times to trade, for example, is when you are feeling down and trying to suppress your problems.

At the same time, losing streaks can lead to depression. This can also lead to the so-called anchoring bias, the tendency to interpret the future by referring to the past. Some traders tend to ignore the fact that market conditions keep changing all the time and keep complaining about their past losses.

The attribution of blame and trading

When our trading strategies fail, it is normal to feel disappointment and sadness. However, when we begin to doubt our abilities to be successful in life when we start to blame ourselves for factors we cannot control, it is evident that we are unable to control our emotions.

Blaming ourselves for our losses can only lead to extreme feelings of guilt, which can be unproductive. After all, markets are full of possible outcomes, not certainties. Unsurprisingly, good traders are the ones mentally prepared for the worst.

How to control emotions while trading?

Although experience, knowledge, and risk management are all factors to consider when trading, they are the foundations of trading psychology that can help us become successful traders. As stated above, profound

emotional experiences can cloud our decision-making strategies, so emotional training is key.

To escape the traps of your mind, you should have realistic observations of the overall market situation. So here are some tips to help you manage your emotions and improve your decision-making strategies during trading:

- Take a break. When you feel overwhelmed by emotions and insecurity, it is best to take it. Engage in behaviors that can help you move forward. Take a walk after a trade, for example.
- Don't trade out of greed or other intense feelings . Cryptocurrency trading is a complex art to master. Don't forget that emotion-based trading can lead to huge losses. After all, since trading is full of changeable possibilities and factors, it requires proper risk management strategies. Online trading is not a gamble or an easy way to make money quickly!
- Participate in Emotional Training Sessions. Only when you are fully aware of your flaws can you become a better

trader. Patience, discipline, and objective reasoning are three vital qualities to help you become a professional in the industry. While it takes time to evaluate your trading strategies, it is worth it.

- Develop Realistic Trading Plans. While cryptocurrency trading can give you an adrenaline rush, we need to stay realistic. Developing an objective work plan, in addition to maintaining a realistic attitude, can help us master the art of cryptocurrency trading. As the market is constantly changing, we cannot expect thousands of euros in our trading account. Realistic expectations are the key to successful trading!
- Learn to move forward. Being obsessed with trade is a big mistake. Don't forget that moving decisions stop losses, and profit levels can only add fuel to the fire. Stop looking at the charts, do something during the most volatile period of the trade. Accept that losing and winning go hand in hand and understand that the market is characterized by changing conditions.

Chapter 46 - Understand your Psychology

Behavioral finance states that investors are subject to various perceptual, mental, and social pressures that lead them to make sub-optimal judgments and undermine their success in the markets and elsewhere when they behave in an 'irrational' way. People can correct or compensate for these deficiencies in human actions and decision-making through their understanding. It also means that markets are not as competitive as conventional wisdom suggests, allowing smart traders to benefit from incorrect pricing.

Keep in mind that while the studies quoted in this chapter refer to stocks and more "traditional" assets, the same conclusions can be drawn for the cryptocurrency market.

Traditional economic theory states that when making investment choices, consumers are rational and consider several variables. Thus,

while we would all prefer to think that investing in certain stocks is a good choice, those who have done so will prove otherwise.

Many factors influence our investment choices. Behavioral finance is the study of the social and emotional biases that cause investors to make unreasonable decisions. Individual investors, fund managers, and financial advisors are also affected in the same way.

Suppose you think investing in the cryptocurrency market is just a matter of statistics. In that case, you will be shocked to find that your psychology is just as significant, if not more so when it comes to making essential choices. The analysis of the mind and action applied to how we spend fascinating and very beneficial for investors. Since market movements are unpredictable and irrational, self-awareness can help us recognize when our instincts are not based on sound reasoning. Nothing is more tragic than wasting money while having the required analysis at hand, simply because of our

natural propensity to behave and think in these aspects.

Investors' thinking assumptions are an essential topic that stock market psychology investigates extensively. Prejudice is an imperfect form of thinking that we have come to accept. Take, for example, the loss aversion bias.

Losses elicit a stronger reaction from investors, hence profits. Consequently, the thrill of earning a profit of $15,000 pales compared to the agony of losing $5,000. This explains why, as the cryptocurrency prices collapse, most investors fear and sell their coins. And, as more people get into the frenzy, the market collapses.

Remember availability and confirmation distortion. Investors prefer to rely on details and knowledge that are easily accessible to them while investigating a company. Thus, investors focus their investment thesis on more information they don't need to dig into rather than looking for valuable but hard-to-

find evidence. Furthermore, once they already have an opinion, they focus on the evidence that supports it, discarding any data that contradicts it.

Since feelings take precedence over thought, we may respond too quickly, too slowly, or not to new market conditions. Yet, according to BMO's recent Investment Psychology survey, two-thirds of Americans cannot control their impulses while making cryptocurrency investment choices.

Dalbar, a financial services consulting firm, published a survey called 'Quantitative Investor Behavior Analysis' in 2001, concluding that ordinary investors regularly struggle to outperform market indexes. For example, the S&P 500 returned an average of 16.29% per year from December 2000 to December 2001, compared to only 5.32% for the median equity investor over the same period: an incredible 9% gap. It also found that the typical fixed-income holder raised only 6.08% per year simultaneously. In comparison, the long-term government bond

index returned 11.83%.

Dalbar argued in a 2015 follow-up to the same publication that ordinary investors struggle to generate market index returns. It was found that 'By a large margin of 8.19%, the typical equity mutual fund investor underperformed the S&P 500. The return on the broader market was more than double that of the typical equity mutual fund investor. equity investment (13.69% versus 5.5% total). Average fixed-income mutual fund investors consistently underperformed the benchmark bond market index, yielding 4.81% lower.

Factors that influence investor psychology

The most challenging problems we face as cryptocurrency investors are those we are not aware of. Some human tendencies affect our investments, but we are always unaware of how they affect our profits. While there are several human traits, we will focus on three that, if not addressed, will hinder our progress

towards our financial goals.

We have no idea who our enemy is

When we approach cryptocurrency investing objectively, we will see where we went wrong and try to correct it in the future. For example, we may change our exit conditions for longer by using a different indicator if we exit a transaction too early in a transfer. When we have a solid trading strategy but are still losing funds, we need to examine ourselves and our psychology to find a remedy.

When we are dealing with our brains, our objectivity is always distorted. We cannot objectively solve the problem because the superficial assumptions and platitudes obscure the real problem. A cryptocurrency trader who does not adhere to a trading strategy but does not recognize that 'not respecting it' is the problem, so constantly changes plans, assuming that this is where the fault lies, is an example of this.

The power lies in becoming aware of the problem

While there is no one-size-fits-all solution to all of our problems, being aware of any potential root causes helps us continue to monitor our thoughts and behaviors to improve our patterns over time. In addition, being aware of possible psychological pitfalls will help us improve our behaviors and potentially increase our earnings. Let's take a look at three different personality quirks that can lead to these problems.

Bias caused by “common sense”

In specific ways, we use the knowledge surrounding us to form an opinion or prejudice, which helps us work and understand. First, however, we must recognize that while we may think we base our decisions on credible facts, we often are not. For example, suppose a cryptocurrency trader follows the news every day and concludes that the cryptocurrency market is rising based on all available data. If so, he may believe that he has come to this

conclusion by ignoring the opinions of the media and listening only to the truth. However, this cryptocurrency trader can run into a problem: his bias is skewed too because his knowledge is skewed.

Furthermore, the evidence can be used to support a bias or an argument, but we must keep in mind that there is still another side to the story. Furthermore, repeated exposure to a particular perspective or belief can lead people to conclude that it is the only viable position on the issue. They would be affected by the relevant facts when they are devoid of counter-evidence.

Explore every possible scenario

Avoiding what might happen or doesn't appear evident to us, often recognized as fear of the future, prevents us from doing certain things, which could trap us in an unprofitable environment. While it may seem absurd to others, traders may be afraid of losing capital. Traders are also thinking about expanding

their comfort zone or fearing that their income will be devoured by taxes as if they are unsure. This would almost certainly involve self-sabotage. Another cause of injury can be trade only with the sector you are most familiar with, even if this sector has been in contraction for some time and should continue. Due to the risk inherent in the investment, the trader is preventing a result.

Another typical mistake is to hold the losers too long when selling the winners too soon. Since the values fluctuate, we must consider the extent of the transition to decide whether the variation is related to noise or a natural consequence. Exiting trades too early is often the product of buyers taking a risk-averse approach and misunderstanding the stock model. On the other hand, when investors lose money, they also become risk-takers, culminating in a long-term loss situation. Thanks to psychological biases, these deviations from rational behavior contribute to unreasonable decisions, leading investors to lose future earnings.

Anticipation is a difficult beast to tame

Waiting is a powerful emotion. Anticipation is often linked to an 'I would like' or 'I need' mentality. This is because we expect something to happen in the future. However, the feeling of anticipation is now, and it can be a pleasant emotion. It can be so satisfying that we pause to enjoy the wait rather than doing what we expected in the first place. Knowing that a million dollars would appear at your door the next day will fill you with hope and anticipation. It is possible to become 'addicted to this feeling.

When items aren't that easy to find, we may fall into the trap of using the feeling of expectation as a consolation reward, seeing billions of dollars changing hands every day but not having the courage to stick to a schedule and taking a cut could indicate that we have subconsciously decided that daydreaming about earnings is enough.

Chapter 47 - Becoming a Better Cryptocurrency Investor

Diversifying your cryptocurrency investment portfolio is the best thing you can do to become a better cryptocurrency investor. Rather than limiting your investments to Bitcoin, investors need to explore other altcoins on the market, as stated in the previous chapters of this book. Furthermore, diversifying the portfolio by investing in multiple cryptocurrencies will allow investors to hedge the potential risks involved. By investing in altcoins and tokens other than Bitcoin, investors can stabilize their earnings more quickly. But it is also essential to invest in cryptocurrencies that have high future potential by doing thorough research.

Furthermore, diversifying your portfolio is also essential for any healthy cryptocurrency profile to explore the space more. For example, suppose you have a specific amount

of funds in all the currencies you trade. In that case, there is less chance of sustaining total losses on your investment during a sudden market fluctuation.

The cryptocurrency market has also received enormous attraction from the public and the media. There are multiple news, information, and articles on social media channels and entertainment platforms. Many investors find themselves swayed by provocative news articles, which often do not provide the accurate and necessary information. This will ultimately result in reckless investments based on completely uncertain and biased opinions. It also further induces investors to make emotional decisions that lead to losses. Therefore, like any other traditional investment, ignoring the hype and filtering out useless news is of the utmost importance.

The best way to become a better cryptocurrency investor is to do your bit of research, be patient, rely on the correct knowledge of trading, investment strategies, and collect the tokens that suit your budget

and degree of risk. A smart way is to thoroughly study the market, tokens and use knowledge to take calculated risks. Therefore, ignore the unnecessary hype around new cryptocurrencies and ask for advice from people who have experience in the sector.

Do your due diligence

Today we live in the modern digital age. Obtaining accurate information and enlightening with the appropriate knowledge is a simple task. Hence, there is no excuse to invest with little or no understanding of the underlying concept of blockchain technology and digital assets. The best way to become a better investor is to access the online whitepapers for each digital asset. The whitepaper will include details such as the developer's plans, specific timelines, significant characteristics of the token, and a general overview of the entire project. Reading the whitepaper carefully will give investors an idea of the project and its future potential to some extent.

Also, suppose the white paper seems incomplete or even misleading. In that case, it exposes a fundamental problem with the project itself, often hostile. For seasoned traders, for most niche investors, cryptocurrency whitepapers will help brush up on their knowledge of potential future investments. However, suppose it fails to convey how the currency is suitable for investors to obtain a good return. In that case, it is always better to look for another investment opportunity.

Always have a detailed investment strategy

Most cryptocurrency investors are opportunistic impulse buyers who invest without a specific plan. However, if you want to become a better crypto investor, a detailed investment strategy is essential. First, always plan why you are in the industry. For example, ranking your strategy according to your investment mandate, whether you are a short-term investor, active or passive, what are your favorite currencies, etc., would be a

good start. Also, plan your budget and initiate specific risk management plans, ensuring fewer losses and greater chances of good returns. Your cryptocurrency investment won't be compelling enough without a protection plan. Therefore, it is essential to have a detailed strategy before entering the market. This will help you know where you are headed with your hard-earned cash and effectively deal with sudden wins and losses.

Be prepared for the unexpected

The cryptocurrency market is highly volatile, which means the chances of sudden turmoil are greater. Therefore, one of the best ways to become a better cryptocurrency investor is to expect the unexpected. Experienced and professional cryptocurrency investors are used to huge swings and take steps accordingly. However, there are various methods to manage a cryptocurrency market crash effectively. Mentally preparing for

these unfavorable situations and adopting practices, such as buying after a collapse, will help investors to act rationally instead of emotionally in moments of unexpected drops.

Chapter 48 - Learning from your mistakes

There is not a single cryptocurrency trader who has never suffered losses in his entire career. Whether due to lack of education, lack of discipline or emotional intelligence, series of bad decisions, or just plain bad luck, every trader will eventually suffer a loss or even several. It is undoubtedly an unpleasant experience that will leave any trader shocked and very disappointed, primarily if he had achieved excellent results with a demo account before this.

Many traders have even quit trading because they have lost money. That is why it is essential to know how to cope with losing money and bounce back after a significant loss. It is necessary to talk about this issue because experiencing a consequential loss can make you doubt yourself. Questioning yourself, career choices, and level of understanding can lead to quitting, skipping trades for fear of losing, or entering more

trades than you should try to get your money back.

Recovering from a significant loss isn't that hard. There are several steps you can take to make things better for you. Of course, these steps can't turn back time and get your money back. However, they can help repair the mental damage done, especially to your confidence.

Change your mindset about mistakes

We all make mistakes. Whether related to our career or personal life, your choices can't always be perfect or right. We are human, after all. See the big picture here; be a bigger person than your mistakes. Many people fall victim to their mistakes, thinking that their failure will define their lives and haunt them to the end of time. That's not true, and the faster you get rid of all these negative thoughts, the better.

Changing your mindset about cryptocurrency trading mistakes will only help you overcome them as quickly as possible and focus on the future. Eliminate the fear of making the same mistakes and try not to get stuck every time you sit in front of a computer and start looking at the graphs. We know it might be difficult, especially the first few times you make a mistake and lose money. Still, suppose you've decided to become a trader with the idea that you'll never make a single wrong move and become a millionaire in no time. In that case, trading probably is not for you.

Analyze your mistake and learn from them

This is probably the best advice anyone can give you on how to get over the shock after losing money in cryptocurrency trading. Simply put, accept that you made a mistake, take your time to deal with the shock and stress, and go back to analyzing what you did wrong and how you can improve it next time.

Start with your strategy. Are you sure you've done everything right? Is there a way to improve it? How about adopting a new one? For novice cryptocurrency traders doing this is an absolute must, but it is also valid for experienced traders. However, professional traders will more easily identify their mistakes and recover faster because they have suffered losses multiple times and are used to this idea.

Beginner cryptocurrency traders should get into the habit of keeping a trading journal. Write what you did wrong, what you thought you did well, how you felt and what significant conclusions you can draw from the whole experience.

What is in the past remains in the past

This is a philosophy that will help you a lot, especially in your trading career. In an environment where things can change in the blink of an eye and where risk is everywhere, you must learn to be resolute, eliminate

emotions and not dwell on the past.

Sooner or later, you have to start cryptocurrency trading again. The faster you recover from your first losses as a beginner trader, the better. After a losing streak, start small and be highly cautious. Don't go back to the same size as the position you traded earlier. You are trying to win back your trust. Having a winning day with a small position will help you do that. You can increase the size of your position the next day.

What we are trying to say is to return to cryptocurrency trading at a slow pace. Increase your position size when you have winning days. We understand it might be frustrating to start with small positions after trading more significant positions. Still, it's better to be safe than sorry, right? Suppose the initial loss was too substantial and you feel badly beaten. In that case, it is essential to dedicate at least 1-2 days to recharge, take a moment to rest, and come back stronger.

Don't rush into trading again after a

significant loss. It would help if you felt ready mentally, strategically, and financially. You will only lose more, repeat the cycle, and you will never recover. One last thing: recovering from a loss does not mean getting your money back as quickly as possible. It's about going back to basics, implementing strategies better, and building experience. Then, when you start rebuilding your trust, the money will come.

A great way to make sure you do not make the same mistake more than once is by keeping a trading journal. And that is what the next chapter will tell you all about.

Chapter 49 - The Importance of Keeping a Cryptocurrency Trading Journal

In its simplest form, a cryptocurrency trading diary is a 'book' that a trader keeps about everything that happens at work and the thoughts that come to his mind concerning his trading experiences.

Most cryptocurrency trading journals record trades and contain specific information relating to what cryptocurrency was bought and sold. This can also result in data points that include the entry and exit price, the quantity traded, the basis for taking that position, and those details. It can also include the goal, the stop loss, and even notes that record insights and actions for the future.

There is no preset format or template for a trading journal. Instead, cryptocurrency traders share many practical examples. Still,

ultimately it comes down to what you are trying to get out of it and how you want to structure it. A cryptocurrency trading journal can be structured and highly customizable but, for best results, it should contain the most essential and impactful data and information to facilitate future trading.

As a busy cryptocurrency trader who has to constantly update on information and data, trends and charts, as well as the hectic pace of trading itself, why should you keep a trading journal? So why do intelligent traders put the time and effort into making sure they regularly log into all their trading activities and refer to them?

There are many benefits to keeping a cryptocurrency trading journal, and here are some compelling reasons you should too. The value of trading journals can best be understood from these apparent benefits they can reap if you keep them diligently.

These are the main advantages offered by the cryptocurrency trading journal.

Acquire and record data and events

One of the most significant benefits of a cryptocurrency trading journal is the essential ability to capture and record all actions performed during a session or day. Thus, this journal is the first-hand archive of all the operations you have performed during a period and can be the ideal reference material for you in the future. It is the type of library that you can build little by little, day after day, which can be a gold mine of information later on.

Take notes and observations

The personal level notes and observations you make there are what sets a cryptocurrency trading journal apart from the widely available charts and general data. This nuanced and insightful database adds a significant degree of intelligence to all generic information.

The more detailed and structured your

comments are, the better the net output you can deduce. These may be of more value for your future trading than many market reports and analyses if done right.

Review, identify and learn from experience

With so much data and information in one place, this becomes the perfect collection of your trading history, complete with successes and failures, highlights, and low points. This can be the best learning and review material you can refer to to get insight into what you did well and review decisions that didn't go well. It's like having your coach and mentor guide and correct you on wrongs while allowing you to motivate yourself on rights.

It helps in self-assessment and in defining goals

A cryptocurrency trading journal is a proper document to refer to when evaluating yourself and your performance. For example, are you constantly growing both in terms of

profits and volumes? How much are you improving with loss containment and risk management? It's all there in the trading journal and can give an excellent and fair assessment of your progress.

Likewise, as a next step, it can also provide you with a future roadmap by evaluating your performance so far and giving direction on new goals. How much more can you take on without risking your capital? What should be the natural trajectory of your goals based on the learning and achievement curve so far? In short, the trading journal can be your mentor and even your boss!

Avoid mistakes

Another priceless benefit that a trading journal offers you is providing insights when you make a mistake or are about to create one. From the previous entries, you can look for similarities of a present situation compared to the past. This is like having a much more experienced colleague or even a mentor who advises you to correct your

course if things go wrong.

Identify trends

A well-kept trading journal is filled with data and information. This can be a treasure trove of intelligence that can show the way forward by spotting trends and capturing patterns. In addition, this feature can generate opportunities that might otherwise be missing from the hustle and bustle of the trading action.

Share your emotions

Of course, keeping a journal is a great way to release pent-up feelings. Hence, a trading journal can also be the perfect outlet for all those emotions - positive and negative - so that you can return to the next trading day completely relieved of them. These observations can also be a source of motivation and learning, depending on whether the voice was from an instance that was a success or a failure.

What are the challenges of keeping a cryptocurrency trading journal? First, let's take a look at some reasons why people refrain from keeping a trading journal.

Consistency

While keeping a journal is one of the critical factors in a trader's success, day traders or short-term traders find it challenging to keep a journal just because it takes time. But, it also makes sense to think, how should you keep a diary when you are in the thick of the action? On the contrary, it could be counterproductive and lead to missed transactions when the opportunity arises.

You don't have to write down every single trade you conduct, but instead, take note when something significant occurs so that you can look back at your trades and evaluate what worked and what didn't. Instead of a handwritten journal, you could even take screenshots of your daily trades, organize them in folders, and review your trading history.

It's not always good news

Many traders fail to sustain a trading journal due to the failures and mistakes in their trading journey. Instead, you need to make observations, identify trading mistakes and not commit the same ones again in the future.

How to set up a trading journal

Given the practical nature of a cryptocurrency trading journal and to get the most out of its maintenance, there are still a few steps to set up and run it. Getting started with creating your trading journal is quite simple. In its most basic form, you could set up a well-thought-out and structured Excel spreadsheet. But then, there are many tools and software available today to help you get a more sophisticated, ready-made version.

Once you have set up the trading journal according to your needs, it is time to consider the aspects to keep it diligently. Here is a general pattern that can be followed to keep your diary:

- Record the operations carried out: enter all the operations carried out, the time of the transaction, the entry and exit price, the size of the process, the objective and the stop loss, and other points of relevance.
- Include Supporting Charts: To support the data points, the trading period chart gives a graphic character to the details. Technical indicators and trend lines can provide a more visual background here. Exit and entry points, as well as support and resistance levels, can also be helpful.
- Add value to the trading diary by inserting notes. Along with the numbers and images, it will be helpful to add a little more plot in notes. Having some of your thoughts and observations can personalize the journal entry that can be valuable later on.

A well-kept cryptocurrency trading journal containing details - data, charts, and notes - of your trades can significantly help a trader increase his chances of success and reduce

risk. But, of course, getting the most value out of the trading journal also depends on how well and frequently the journal is reviewed and some practical insights derived from it.

Chapter 50 - Why Beginner Cryptocurrency Traders Do Not Make Money

Why do most beginner cryptocurrency traders fail? It is known that anyone can learn to trade and earn from this activity. However, why do over 80% of cryptocurrency traders lose money? These are the reasons why a novice trader loses money.

Cryptocurrency trading is a profession, and as such, anyone who wants to learn and get results knows that he must strive to learn the skills necessary to be successful. Here are three beginners tips to stay ahead of the game.

Be impatient

Most novice cryptocurrency traders cannot control their temper and are unable to trade their system with discipline. A common

mistake of novice cryptocurrency traders is not to accept losses. Losses are part of cryptocurrency trading; even the best traders in the world close some trades at a loss. To be successful, you must learn to accept losses quickly and keep them small. The cryptocurrency market continually offers opportunities, and recovering losses, if you keep them small, can be accessible by following your trading plan.

Trading without having a trading plan

Having a trading plan is essential; it is the first step to success. Experienced cryptocurrency traders follow in detail a trading plan that includes risk management and specifies the expected return on investment (ROI). The cryptocurrency trader who operates without a trading plan is like trading in the dark; it will be impossible for him to be successful trading this way.

Bad risk management

Cryptocurrency traders should focus and exert all their efforts on risk management as well as developing a sound strategy. Mismanagement of risk is the root cause of every cryptocurrency trader's failure.

So, let’s talk about risk management.

Financial investments carry a certain degree of risk. For this reason, before investing in cryptocurrency, every person must be very clear about the threat they are facing and have a method for managing risk. Unfortunately, perhaps not many people use a risk management system in their investments, which is why many people lose money on cryptocurrency investments.

Risk management is an investment technique that aims to maximize profits while limiting losses as much as possible. This technique is used in investment management, and some decisions may result based on the uncertainties of the present situation. More precisely, risk management concerns the percentage or part of the economic well-being

of those who decide to invest. In this sense, therefore, risk management not only performs a portfolio protection function but also has the function of speeding up the investor's choice in choosing the most suitable investment.

The risk management technique is used in investments and gambling. It allows you to manage money with greater control over gains and losses. Risk management plays a fundamental role if we refer to assets and should be integrated into your cryptocurrency trading strategy. Risk management does not involve making only winning investments; making a trade at a loss happens to everyone, but you can maximize your profit and minimize your losses if you use it correctly.

Chapter 51 - Beware of Scams

Cryptocurrency scams are plentiful and can cost investors dearly. Here's how to spot them.

Verify the existence of the blockchain

Cryptocurrencies operate on blockchain networks. It is not necessary to know exactly how a blockchain works. Still, it is essential to understand that without it, cryptographic tokens cannot exist. Scammers like to hide their fraud by claiming that their blockchain is 'in development' or 'about to be released. The OneCoin scam is a great example. According to a BBC investigation, OneCoin executives said they kept their blockchain on their computers.

Any legitimate blockchain will have an accompanying website that allows you to explore or scan transactions to verify their

existence. Type the token name and 'blockchain explorer' or 'blockchain scan' into a search engine to find it. Suppose the token has its blockchain network (or is operating on Ethereum). In that case, you should see if things are going well there, with lots of recent activity.

Pay attention to the suggestions of your 'friends'

Multilevel marketing, or MLM, scammers typically use the language of cryptocurrencies to get people to bring their crypto-curious friends to their pyramids, promising them bonus payments for recruiting more 'members.' But crypto projects don't have 'members': they have investors. And in most cases, bringing in friends and family doesn't bring in money. MLM experts know that being at the top of the pyramid is a quick path to wealth. But getting involved in the lower levels could be a quick way to financial ruin. Last year, a US court convicted a California man who deceived investors worldwide for $ 147 million. He was running a pyramid

scheme that promised members access to tokens, Bloomberg said.

Don't listen to cryptocurrency advice from a long-lost cousin or a former workmate who just befriended you on Facebook. Instead, go to price-tracking websites like CoinMarketCap, CoinGecko, or CoinPaprika and look for large-cap coins (or promising small or mid-cap cryptocurrencies, if you prefer). These sites contain historical and real-time data on coin prices and trading volumes. If the token Cousin Jimmy is talking about isn't listed on any of these monitoring platforms, it's very likely a scam.

If someone starts talking to you about 'guaranteed' returns, run away

There is no security in cryptocurrencies. Scammers who claim to have developed high-tech solutions that can guarantee investors' earnings usually end up behind bars. For example, four employees are

currently on trial in Japan to run an 'artificial intelligence' scam. According to the Japanese newspaper Asahi Shimbun, the scammers had devised a scheme that promised investors to double their investments in just four months, claiming that their artificial intelligence robots could spot winning trades in real-time. But angry investors claim that the robots did nothing of the sort and that investors' funds in the project were lost. No supercomputer, artificial intelligence tool, or magic wand can guarantee anything in the crypto world. So if someone claims that he can remove the element of risk from cryptocurrencies, he is trying to scam you.

BONUS CHAPTER: Cryptocurrency Debit and Credit Cards

Although much of the interest in the crypto world is related to investment potential, this ecosystem still brings other benefits, such as the transfer of value. Satoshi Nakamoto didn't create Bitcoin to make people billionaires. Instead, Bitcoin was designed as a digital and global payment system. One way to achieve this is through the use of crypto cards. This payment method is helping people to use cryptocurrencies and digital assets in their daily lives and receive crypto rewards.

A crypto card works in a similar way to your debit card. You can pay for goods or services, which your card provider accepts. While it may appear that you are paying a seller directly with digital currencies, this is not precisely what happens. The seller receives fiat money in their account and not in cryptocurrency. Your crypto card takes the

cryptocurrency from your account, converts it to the local currency you're paying in, and then uses these funds to pay. We will explain this later with an example.

Both Visa and MasterCard offer crypto cards to partner companies that require a license. These two are the most popular payment service providers globally, which makes crypto cards almost universally accepted by all retailers. Some crypto cards only offer rewards on the money spent with such cards. These are generally credit cards, which require a credit check to be applied for.

As mentioned, a crypto card doesn't pay a seller using cryptocurrencies. Conveniently convert your cryptocurrencies into cash, with which you can pay a seller via card.

For example, imagine you have $500 in a crypto card issued in your favorite exchange. Let's say you use the Binance card. At a restaurant, you pay the $100 bill with your crypto card. After inserting your card and accepting the payment, Binance sells $100

worth of crypto and loads the fiat funds to your card. The restaurant then receives $100, and you have another $400 left in your funding wallet. All this happens in the few seconds you use your crypto card.

You can also use these crypto cards to withdraw at ATMs if your service provider supports this feature. The same method described above is used to withdraw physical cash.

Differences between a crypto card and a credit or debit card

There are some minor differences between credit/debit cards and crypto cards. But, for the most part, they work the same way when making payments. The most significant difference between a crypto card and a credit/debit card is that the former top it up with cryptocurrencies. A debit card is preloaded with fiat currencies, and credit card transactions are settled with fiat currencies.

A crypto prepaid card works in a similar way to a traditional debit card. You must have

funds in your account before you can spend them. You cannot load your card with a fiat currency but only with cryptocurrencies. When you make a payment, your funds are instantly converted within your crypto wallet.

At the same time, crypto credit cards provide a line of credit that allows you to buy now and pay later. Gemini and BlockFi have both released crypto credit cards with related cryptocurrency cashback. You can settle your credit card bill using fiat currency, which means that the crypto credit card is a credit card that provides a reward.

To order a card, you will need to be a customer of a company that already provides a crypto card, such as an exchange or a bank that supports cryptocurrencies. The process will involve completing Know Your Customer (KYC) and anti-money laundering procedures before you can order your crypto card, just like before you call a regular credit or debit card. With a crypto credit card, you will also need to pass a credit check.

Advantages of a crypto card

The main advantage of a prepaid crypto card is the ability to use cryptocurrencies for your daily purchases. However, it is usually challenging to use cryptocurrencies to pay unless a seller accepts a crypto payment directly. Even if this were the case, some coins like Bitcoin could take up to 30 minutes to confirm a transaction. Also, take into account the volatility of the price. This means that you may be paying more or less than expected.

Many crypto cards also offer various benefits such as rewards through a cashback mechanism or discounts on certain subscriptions such as Spotify or Netflix. These benefits will direct you to a specific card provider. Those benefits are similar to those offered by standard debit/credit cards. Make sure you compare the offers available for each card to find the one that works best for you. Also, don't forget to check any exchange fees you may have to pay during the conversion process.

Do crypto cards have any risks?

Having a crypto card has the same risks that one can be exposed to owning cryptocurrencies. For example, if you have loaded your account with Bitcoin (BTC) or Ether (ETH), the fiat value of your account will change constantly. This means that you may not have the exact amount of money you think you have in your account, as this varies based on exchange rates.

You should also bear in mind that spending cryptocurrencies lead to a taxable event in many tax jurisdictions. It doesn't matter if you spend a few dollars on a coffee or thousands of dollars on a car. Suppose you have made any gains or losses with your cryptocurrencies. In that case, you will need to pay or deduct the appropriate taxable amount before using them to purchase anything with your crypto card.

You can avoid this problem by purchasing stablecoins to use with your crypto card, as their price rarely changes from the underlying

value they are related to.

Conclusion

Here we are at the end of this journey. As you might have guessed, investing in cryptocurrencies is not that complicated if you follow a strategy and a rational approach. Indeed, 2021 is crucial for this sector, thanks to the institutional interest created mainly around Bitcoin. This is excellent news for you who has now read this book. While most people are still hesitant and waiting for the "right time" to enter the market, you have the opportunity to start your advanced accumulation plan, ensuring you get a head start on the competition.

The next step is to practice what you have learned in this manual without deviating from the strategies taught. It is only by investing with perseverance and a precise plan that you can achieve significant financial satisfaction.

Check List Cryptocurrency Evalutaion

Cryptocurrency name: _____

Ticker:_____

Today's date and price:_____

Historical high and date of when it was marked:_____

Capitalization:_____

Project’s goals:_____

Notes:_____

- It is tied to Bitcoin.
- It offers greater return potential than Bitcoin
- It has at least a capitalization of $40 billion

- It is not a stablecoin
- It has lower internal inflation than the legal tender you are using as a reference.
- It does not make deflation its sole strength.
- 50% of the money in circulation is distributed among at least 50% of the investors
- It does not require trust in an external company or entity.
- It has been on the market for at least three years and has survived a bear market.

Glossary

Altcoin: any cryptocurrency other than Bitcoin.

Asset: any 'thing' that can be bought and holds or increases its value over time.

Bitcoin: a digital form of money that is decentralized, censorship-resistant, secure, and borderless.

Blockchain: is a database, visible to everyone, in which all transactions are recorded. Transactions are grouped into blocks; these blocks are cataloged chronologically.

Capitalization: indicates the amount of money present in an asset. It is calculated by multiplying the unit price by the total working capital.

Diluted capitalization: Indicates the amount of money in an asset weighed against the amount available in the future. It is calculated by multiplying the unit price by the maximum number of units that will ever be

on the market.

Private key: the part of the address known only to its owner, allowing transactions to be carried out. It can be thought of as the home banking password.

Public key: the part of the address that publicly identifies a user's wallet. It can be thought of as the IBAN of a current account.

Diversification: a strategy aimed at reducing the financial risk of one's investment portfolio.

Exchange: is a platform that allows the buying, selling, and holding of cryptocurrencies.

Halving: in Bitcoin, this event splits the reward that miners receive for validating blocks.

Address: is the location from and to which funds are sent.

Consensus mechanism: is the process used by a blockchain to validate its blocks. The two most famous are mining and staking.

Simple moving average: a statistical

indicator obtained from the arithmetic average of the price of an asset over a given period.

Memecoin: is a cryptocurrency that has no purpose other than to create humor around itself.

Mining: the process by which blockchains with a Proof of Work consensus mechanism validate blocks.

Portfolio Rebalancing: a six-monthly process whose task is to bring the asset allocation back to the values established by the investor at the time of portfolio creation.

Stablecoin: is a cryptocurrency that aims to maintain a value as constant as possible.

Staking: is a process of earning a return on one's capital by blocking funds and validating blocks on a blockchain. However, not all cryptocurrencies use staking as a consensus mechanism.

Wallet: is what allows you to store the private keys of one or more addresses. It can be 'hot' if it relies on the internet and 'cold' if it holds the keys offline.

Useful Resources

Buy and sell Bitcoin and other cryptocurrencies:

- coinbase.com
- youngplatform.com
- www.therocktrading.com
- www.binance.com

Find a hardware wallet that's right for you:

- www.ledger.com
- trezor.io

Monitor the performance of your favorite cryptocurrencies:

- coinmarketcap.com

Stack your ADAs:

- yoroi-wallet.com

Profit from your ETH and BTC:

- blockfi.com
- crypto.com
- nexo.io

Keep track of your portfolio's performance:

- cryptocompare.com

References

- warrenbuffettstockportfolio.com
- hedgefollow.com
- coinmarketcap.com
- academy.binance.com
- ycharts.com/indicators
- reddit.com
- ledger.exposed
- bscscan.com
- binance.com
- coinbase.com
- cryptonews.com
- therocktrading.com
- youngplatform.com
- trezor.io
- ledger.com
- sfoerster-5338.medium.com

- broadridgeadvisor.com
- finder.com.au
- yoroi-wallet.com
- daedaluswallet.io
- blockfi.com
- nexo.io
- crypto.com
- cryptocompare.com